CHAPTER – IV
WORLD WIDE IMPACT OF CYBER CRIME AND INDIAN LEGAL RESPONSE

Human civilization has witnessed a significant development in last decade. The dawn of the new millennium have suddenly changed the words of the 19th century. Whole world is undergoing a technological change. As human civilization develops, new questions and problems crops-up. This problem brings with it social, economical and especially legal challenges. Law must keep pace with these challenges. It must respond to the cry of the community that it is there to serve the needs of the society. New challenges ask for new solutions and to resolve such problems law must be flexible enough to meet the ends of the justice.

The revolution brought by the Internet and the world wide web is having an immense impact on all aspects of human existence. With the dawn of technological revolution, the whole world has become a global village, whereby the present law enforcement machinery may not be adequate enough to serve its purpose.

However, it is unfortunate that this technological change has brought with it many disadvantages around the globe. And what civilization has found is, that, the present law enforcement machinery has failed in this cyber jungle... The birth of Internet and its rapid growth has brought many complex problems to Governments, individuals and commerce. There is no doubt that such technological change has brought many benefits, but become of its low cost and ease of use, it has also brought with it certain disadvantages at all levels in society.

1. REASONS BEHIND THE INCREASE IN CYBER CRIME

The reasons for the vulnerability of computers may be said to be:-

1.1. Capacity to store data in comparatively small space:- The computer has a unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium much more easily.¹

1.2. Easy to access:- The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. Secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders, retina imagers etc. that can fool biometric systems and bypass firewalls, can be utilized to get past many security systems.

1.3. Complex:- The computers work on operating systems, in turn, are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.²

1.4. Negligence:- Negligence is very closely connected with human conduct. It is, therefore, very probable that while protecting the computer system, there might be any negligence, which in turn, provides a cyber criminal to gain access and control over the computer system.

1.5. Loss of evidence:- Loss of evidence is a very common and obvious problem as all the data are routinely destroyed. Further, collection of data outside the territorial extent also paralyses this system of crime investigation.³

1.6. Lack of Effective Laws Relating to Cyber Space:- Laws, criminal justice systems and international cooperation have not been able to keep pace

with technological advancements. Only a few countries have drafted laws to address the problem.\(^1\)

2. **WORLD WIDE IMPACT OF CYBER CRIMES**

Computer crime virtually affects everyone—individuals, business organizations, government organizations, nation states. It also affects the society and national and international economies. Impacts of cyber crime are as follows—

2.1. **The Global Scenario**

Cyber crime is a worldwide problem that’s costing countries billions of dollars.\(^2\) There is a great concern world over regarding various types of crimes being committed through computers and the internet. Almost every day there is an international story about some or the other portal that has been attacked, credit card fraud, or some virus bringing down the system. Business is the prime target—but public authorities and even individuals are vulnerable too.

Cyber crime has a direct impact on bottom lines, as well as exposing businesses to identity theft, data leakage, privacy liability issues and compromised intellectual property—cyber crime in its various forms—computer crime, identity theft and phishing—costs the U.S. economy some US $117.5 billion a year, according to a Government Accountability office (GAO) report in July 2007.\(^3\)

According to the Congressional Research Service, several computer security consulting firms estimate global financial losses from virus, worm attacks and other hostile computer-based attacks to be between $ 13 and $ 226 billion.\(^4\)

It has generally been acknowledged by the experts that there is hardly any computer in the world that is hacking proof. Cyber crime affects more than the financial integrity of a business. There are many very real and damaging consequences associated with Internet Crime.\(^5\)

---

The Internet Crime Complaint Center (IC3) began operation on May 8, 2000, as the Internet Fraud Complaint Center. Established as a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI), IC3 serves as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. Since inception, IC3 has received complaints across a wide spectrum of cyber crime matters, including online fraud (in its many forms), intellectual property rights (IPR) matters, computer intrusions (hacking), economic espionage (theft of trade secrets), child pornography, international money laundering, identity theft, and a growing list of additional criminal and civil matters.

IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the local, state, and federal level, IC3 provides a central referral mechanism for complaints involving Internet-related crimes. For affected members of industry, IC3 can leverage both intelligence and subject matter expert resources to identify and craft an aggressive, proactive approach to combating cyber crime.

IC3 2009 Internet Crime Report is the ninth annual compilation of information on complaints received by IC3 and referred to law enforcement or regulatory agencies for appropriate action. This report does not represent all victims of Internet crime, or crime in general because it is derived solely from the people who filed a report with IC3.

General IC3 Filing Information:-

Complaints are submitted to IC3 at www.ic3.gov. Complainants without Internet access are advised to use resources at their local library, educational institution, local law enforcement agency, or local victim’s assistance office. After

---

a complaint is filed with IC3, the information is automatically referred to the appropriate local, state, and federal law enforcement agencies.

From January 1, 2009 through December 31, 2009, there were 336,655 total complaints filed with IC3 (Figure 1). This is a 22.3% increase compared to 2008 when 275,284 complaints were received. The number of complaints filed per month, for 2009, averaged 28,055. Dollar loss of complaints referred to law enforcement was at an all time high in 2009, $559.7 million, compared to previous year (Figure 2).

The number of complaints referred\(^1\) to law enforcement has increased from 72,940 in 2008 to 146,663 in 2009 (Figure 3).

During 2009, IC3 implemented a new complaint classification system. This complaint-driven system is based on a logic-driven questionnaire that generates an automatic classification of the complaint into one of 79 offense-based categories. This redesign has also resulted in a number of changes to the way IC3 system gathers and classifies complaint data. The new classification system improves upon the previous system by making clearer distinctions between complaint elements and by reducing the number of categories used to classify complaints.

The results contained in this report were based on information that was provided to IC3 through the complaint forms submitted at www.ic3.gov. The data represents both a complete analysis of all the complaints and a sub-sample of those complaints that have been referred to law enforcement. Although IC3’s primary mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime, those complaints involving other types of crime such as telephone and mail contact were also referred.

---

\(^1\) All complaints not directly referred are still accessible by law enforcement, used for trend analysis, intelligence gathering and consumer education. Typically, these non-referred complaints do not involve a documented case of financial or physical harm or involve a situation in which neither the complaint nor perpetrator reside within the United States. In a minority of cases, there is no designated agency to refer a complaint, based on jurisdictional factors or agency-defined thresholds for referral.
Complaint Characteristics

During 2009, email scams that used the FBI’s name was the offense most often reported to IC3, comprising 16.6% of all crime complaints. Non-delivery of merchandize and/or payment represented 11.9% of complaints. Advance fee fraud made up an additional 9.8% of complaints. Other top 10 complaint categories included identity theft (8.2%), overpayment fraud (7.3%), miscellaneous fraud (6.3%), spam (6.2%), credit card fraud (6.0%), auction fraud (5.7%), and destruction/ damage/ vandalism of computer property, (i.e., “computer damage”, 4.5%) (Figure 4).

The complaints referred to law enforcement by IC3 were largely those cases involving identifiable loss. That meant certain complaints received in high numbers (e.g., FBI scams) were referred in lower numbers because the complaints intent was to notify IC3 of the scam, rather than report a financial or physical loss.
Of the 146,663 referrals during 2009, 100,296 involved a victim who reported a monetary loss. The total dollar loss from all cases of fraud in 2009 that were referred to law enforcement by IC3 was $559.7 million; that loss was greater than 2008 when a total loss of $264.6 million was reported. Much of this increase can be attributable to a greater number of higher loss complaint categories (e.g., identity theft) relative to auction fraud, which historically has been among lowest loss an offence. Of those complaints reporting monetary loss that were referred to law enforcement, the mean dollar loss was $5,580 and the median was $575. The significant difference between the mean and median losses is reflected by a small number of cases in which hundreds of thousands of dollars were reported to have been lost by the complaint. Over 20 percent (21.7%) of complaints referred to law enforcement involved losses of less than $100 and 36.7% reported a loss between $100 and $1,000. Just over 28 percent (28.3%) of the complaints referred to law enforcement reported losses between $1,000 and $5,000 (for a grand total of 86.7% of complaints referred to law enforcement showing a loss of $5,000 or less), and 13.4% indicated a loss greater than $5,000 (Figure 6). The highest dollar loss per referred incident was
reported by overpayment fraud (median loss of $2,500) complainants. Investment fraud (median loss of $1,857) and advance fee fraud (median loss of $1,500) complainants were other high dollar loss categories.

Figure 5: 2009 Top 10 Most Referred IC3 Complaint Categories (Percent of Total Complaints Referred)

Figure 6: Percent of Referrals by Monetary Loss

<table>
<thead>
<tr>
<th>Monetary Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0.01 to $99.99</td>
<td>28.3%</td>
</tr>
<tr>
<td>$100 to $999.99</td>
<td>36.7%</td>
</tr>
<tr>
<td>$1,000 to $4,999.99</td>
<td>6.5%</td>
</tr>
<tr>
<td>$5,000 to $9,999.99</td>
<td>5.8%</td>
</tr>
<tr>
<td>$10,000 to $99,999.99</td>
<td>1%</td>
</tr>
<tr>
<td>$100,000.00 and over</td>
<td>1%</td>
</tr>
</tbody>
</table>
2.2 The Indian Scenario

Computer crimes had not emerged as a major problem area for the law enforcement agencies in India until recent past. The main reason for low incidence of computer-related crimes in India was that computerization of banks and other financial institutions were still in early stages. Further, the networking of computers had not yet taken place in any big way in the sensitive sectors which could be vulnerable to theft and alteration of data. But as the process of computerization has now picked up significant increase in computer crime is expected in the near future. Difficult to detect, seldom repeated and even more difficult to prove, computer-related crime lacks a traditional paper audit trail, is away from conventional policing and requires specialists with a sound understanding of computer technology. Furthermore with the country poised to enter the information superhighway—over three million computers in place and industry and banks networked, the realization of the dangers and threats is finally sinking in.  

The major areas of concern, which are highly vulnerable to the threat of computer crimes, include critical infrastructures like banks and other financial institutions, telecommunications, airlines, railways, power sector and other crucial departments of both the Governments of India and numerous states etc.

India is fast emerging as a major hub of cyber crime as recession is driving computer – literate criminals to electronic scams.

India has risen to the fifth spot in the world's cyber crime ranking for 2009 from the 11th spot in 2008 and now only lags behind the US, China, Brazil and Germany.

The report, compiled by Internet security products firm Symantec, shows that cyber criminals are now increasingly going for web-based attacks using

---

social-networking sites compared to the earlier dependence on the e-mail route used to steal information about credit cards and bank accounts.

Symantec Vice-president David Freer told MAIL TODAY that social networking sites are becoming the target for cyber attackers because these involve a set of like-minded people who trust each other. “It is the cultural trust that cyber attackers find easy to exploit”, he added.

Freer said in 2009 India ranked second in web-based attacks in the Asia Pacific region, which includes China, Australia, Japan and the ASEAN countries, with 16 percent of the total attacks.

This is a significant rise from 2008 when India accounted for less than one percent of web-based attacks in the region.

Globally, in 2009, India ranked seventh with three percent of the total web-based attacks worldwide.

India saw an average of 788 bots per-day in 2009. About 62,623 distinct bot infected computers were observed in India during the period. With 50 percent, Mumbai had the highest number of bot-infected computers, followed by Delhi at 13 percent and Hyderabad at seven percent. “Throughout 2009, we saw botnet infected computers being advertised in the underground economy for us little as three percents computers”, Freer pointed out.

In 2009, spam made up 88 percent of all e-mails observed by Symantec of the 107 billion spam messages distributed globally per day on average, as much as 85 percent were from botnets.

As many as 71 percent of the malicious codes were propagated through file-sharing, 35 percent through file transfer and common Internet file system and 17 percent through remotely exploitable vulnerability.¹

3. INFORMATION TECHNOLOGY ACT, 2000

With the induction of computers in each and every part of our lives, it was not surprising to witness the enactment of the Information Technology Act, 2000.

However, what took many people by surprise was the promptness of the enactment. The Ministry of Information Technology\(^1\) was formed in 1999 burdened with the enormous duty of making India and IT super power by 2008\(^2\). In less than a year, India witnessed the enactment of its first statute relating to information technology\(^3\) on the pattern of the Model Law on Electronic Commerce (UNCITRAL)\(^4\) adopted by the United Nations Commission on International Trade Law. The Information Technology Act, 2000 (hereinafter “the IT Act”) was passed by Parliament on May 15, 2000, approved by the President on June 9, 2000 and notified to come into force on October 17, 2000.\(^5\)

3.1. Premises, Preamble and Focus

The Indian Act was mainly based on the UNCITRAL Model law on Electronic Commerce.\(^6\) The UN General Assembly Resolution adopting this Model law also call upon members to give favourable consideration to the said Model law when they enact or revise their laws, to ensure uniformity of the law across the globe. The focus of the Model law is on the need for uniformity of national laws applicable to alternatives to paper based methods of communication and storage of information and also adoption of reliable electronic records for efficient delivery of government services in the member states. It act as a starting point for identification and discussion of areas where the law could be updated to consider new technology, as well as including certain internationally settled provisions for dealing with those issues and:

---

3 Under the Act, following rules, regulations and guidelines have been framed: (a) the Information Technology (Certifying Authorities) Rules, 2000; (b) the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000; (c) the Information Technology (Certifying Authority) Regulations, 2001; and, (d) the Guidelines for Submission of Application for Certifying Authority, 2001.
4 http://www.uncitral.org/english/texts/electcom/.
5 Notification regarding date of enforcement of the Act “17.10.2000-In exercise of the powers conferred by s. 1(3) of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby appoints 17th Day of October 2000 as the date on which the provisions of the said Act comes into force. [No. 1(20)/97-IID(NII)/F6]”.
• Established Rules that validate and recognize contracts formed through Electronic means;
• Sets default Rules for contract formation and governance of electronic contract performance;
• Defines the characteristic of valid electronic writing and an original document;
• Provides for the recognition of electronic signatures for legal and commercial purposes;
• Supports the admission of computer evidences in Courts and Arbitration of Proceedings.

Since the Indian Act is based on this Model law, it can be seen that its focus is mainly on regularizing e-commerce. It does not focus its attention towards combating cyber crime as such. However, it contains certain provisions that deal with offences falling under this genus.

3.1.1. Object of the Act

The electronic transactions like other parts of the globe, are in vogue in India,¹ however, without legal security.²

The increasing growth of electronic commerce, popularly called e-commerce, made it necessary to have legal protection to such transactions. The Indian Parliament took a step of seminal importance by passing the Information Technology Act, 2000. This Act has three objects that are:

- to respond and give effect to the United Nations call to all states to give favourable consideration to Model Law when they enact or revise their laws so as to facilitate harmonization of the laws governing alternatives to paper based methods of communications and storage of information.

---

¹ The Minister of Parliamentary affairs made announcement, immediately after the Information and Technology Act, 2000 was passed, that in 1990 business worth Rs. 450 crore was transacted through electronic communications and expected business worth Rs. 2500 crore in 2000 through electronic medium HT 16 May, 2000. According to a survey conducted by NASSCOM (National Association for Software and Service Companies), Indian e-business turnover is likely to be around Rs. 450 crore in 2000 and expected to reach Rs. 10,000 crore by 2002, Computers Today, Nov. 30, 1999, p. 17.

² This fact was admitted by the Parliamentary Affairs Minister Shri Pramod Mahajan in Parliament, Hindustan Times 16 May, 2000.
to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly called as "electronic commerce" which involve the use of alternatives to paper based methods of communication and storage of information.

- to facilitate electronic filing of documents with the Government agencies so as to promote efficient delivery of Government services by means of reliable electronic records.

3.1.2. Preamble

The preamble to the Act states that it is ‘An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communications, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker’s Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934, and for matters connected therewith or incidental thereto’. This clearly shows that the focus of the Act is limited to facilitating e-commerce and e-governance and does not include combating of cyber crimes.

3.1.3. Scope of the Act

The Indian Parliament being alive to the ground realities such as lack of infra-structure for new technology, computer literacy and functional equivalents decided to limit the scope of the IT Act and did not extend it to-

(a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;
(b) a power of Attorney as defined in section 1A of the Powers of Attorney Act, 1882;
(c) a trust as defined in section 3 of the Indian Trusts Act, 1882;
(d) a will as defined in clause 4 of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;
any contract for the sale or conveyance of immovable property or any interest in such property;

(f) any such class of documents or transactions as may be notified by the Central Government in the official Gazette.¹

The IT Act extends to the whole of India, including the state of Jammu and Kashmir and has come into force on 17.10.2000.² The provisions of the IT Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.³ It also applies to any offence or contravention committed outside India by any person irrespective of his nationality if that act or contravention involves a computer, computer system or computer network located in India.⁴ The extra territorial ambit of the IT Act is not unusual. The provision giving extra territorial jurisdiction is found in IT specific legislations of other jurisdictions also.⁵ Obviously the need for such provision is driven by the borderless nature of the Internet. These provisions are, however, viable only if there is mutual co-operation amongst enforcement authorities and Government.⁶

4. INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

The Information Technology Amendment Bill 2008 was passed by the Lok Sabha and the Rajya Sabha in the last week of December 2008 and received the President's assent on 5 February 2009. The Bill aims to make sweeping changes in the existing Indian cyber law framework, including inserting new express provisions to bring more cyber offences within the purview of the IT Act 2000. This led to the passage of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act, 2008 has brought marked changes in the IT Act, 2000 on several courts.

¹ Section 1(4) of the IT Act, 2000. This provision corresponds with section 4(1) of the Singapore Electronic Transactions Act, 1988.
² Vide notification No. GSR 788 (E), dated 17.10.2000.
³ Section 81 of the IT Act.
⁴ Sections 1(2) and 75.
without permission downloads, copies, or extracts any data, computer database or information from such computer, computer system or computer network”. The explanation (ii) of the Sec. 43 defines, “database” as, “the representation of information, knowledge, facts, concepts, or instructions prepared in a formalized manner”. Though this section can be applied for electronic databases, its effectiveness is still to be tested for granting protection to databases or data on the Internet.

The aforesaid clause (b) has used specific words, like “downloads”, “copies” or extracts of highlight the ‘software-hardware’ interface involving a computer, computer system or computer network. Any unauthorized “down loading”, “copying” or extraction of any data, computer database are specific acts of omissions that shall make the offender liable to pay damages by way of compensation not exceeding one crore rupees to the prison so affected. It is important to distinguish the terms “down loading”, “copying” and “extraction” vis-à-vis digital content:

**Downloading**: Retrieving a file (digital content) from a remote computer, computer system or computer network.

**Copying**: Retrieving a file (digital content) from a remote computer, computer system or computer network and then saying it on either computer’s hard disk or any removable storage medium.

**Extraction**: Retrieving a file (digital content) from a remote computer, computer system or computer network and then selectively ‘extract’ part of the digital content.¹

**Sec. 43 (c): Computer Contaminant or Computer Virus**

Under clause (c), any person who, “introduces or causes to introduce any computer contaminant or computer virus” shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. Explanation (i) of sec. 43, provides for the definition of a, “computer contaminant”, as any set of computer instructions which are designed to, (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. Explanation (iii) to sec. 43, further provides for the definition of a, “computer virus” as, any, “computer instruction, information, data or programme that destroys, damages, degrades or adversely affects that 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”. This clearly includes with its ambit all the categorizations of viruses listed in the technical background above.

The legislature in drafting this section has kept in mind the difference between authorizing a computer virus and introducing it into a computer resource. This is done for a variety of reasons that includes the difficulty which may arise in tracking the author of a virus. However, this may pose an onerous liability, on an innocent third party who is not aware or does not have knowledge as to the nature of, the infected resource that he may be introducing inadvertently.

Demonstration of actual knowledge is not a prerequisite, to satisfaction of the section. This proceeds on the rationale that the person introducing the virus, will be aware that the introduction of the virus will cause certain damage.1

Criticism of the aforesaid clause has been that the amount of compensation may not commensurate the economic losses incurred by the owner of a computer, computer system, computer network, data, computer database or software on account of disruption in its normal (programmed) activity caused by a computer contaminant or computer virus.2

Sec. 43 (d): Damage to Computer, Computer system etc:-

The aforesaid clause (d) takes into account (i) attempts made to damage or (ii) successful damage, of any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer,

computer system or computer network punishable. Explanation (iv) to Sec. 43, further defines, “damage” as, “to destroy, alter, delete, add, modify or rearrange any computer resource by any means”.

It includes damage to both hardware and/or software either done physically or through a virtual medium. It includes both physical\(^1\) and/or virtual\(^2\) damage to any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network.

The section aims at the providing for compensation in case of harm of the integrity of data. The section thus specifically is enacted to guard against data diddling. Sec. 43(d) is sufficient to cover almost a majority of the cases of damage and mischief that takes place in the context of the electronic environment in today’s context.

Sec.43 (e): Disruption of Computer, Computer system, etc

The aforesaid clause (e) takes into account (a) attempts made to disrupt or (b) successful disruptions, of any computer, computer system or computer network. Disruption here implies unexpected deviation in the normal (programmed)/standard operations of a computer, computer system or computer network.

The disruption more often is caused by DoS attacks. However the section does not limit its scope only to, DoS attacks and the disruption may be caused by any reason. Significantly, the section does not provide for as to minimum period of time for which the disruption must be caused.\(^3\)

---

1 Unauthorized Physical Damage: Implies changing the original/earlier hardware-software configuration of any computer, computer system or computer network; destroying, altering, deleting, adding, modifying or rearranging the binary files (data, computer data base or any other programmes) residing in any computer, computer system or computer network, ‘manually’ and in an unauthorized manner.

2 Unauthorized Virtual Damage: Implies changing the original/earlier hardware-software configuration of any computer, computer system or computer network; destroying, altering, deleting, adding, modifying or rearranging the binary files (data, computer data base or any other programmes) residing in any computer, computer system or computer network, ‘remotely connected’ using satellite, microwave, terrestrial live or other communication media and in an unauthorized manner.

Disruptions may lead to malfunctioning of a computer, computer system or computer network thereby affecting its expected normal (programmed)/standard performance. It is obligatory that the clause (e) be studied/ applied along with the aforementioned clauses (c) and (d) as these clauses may also be one of the reasons of disruption.

Any person who disrupts or causes disruption of any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network shall be liable to any damages by way of compensation not exceeding one crore rupees to the person so affected.

Sec.43 (f): Denial of Access to Computer, Computer System, etc

The aforesaid clause (f) provides for a penalty in case any person, “denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means”. This section specifically prohibits the use of DoS\(^1\) and/or DDoS attacks. The section is attracted to an act if, (a) there is a denial of access; (b) to a person who is authorized to such access; (c) to any computer, computer system or computer network; and (d) by any means.

Sec. 43 (g): Assistance for unauthorized access

The aforesaid clause (g) is an attempt by the legislature to create an obligation for the users. The sweep of the clause is quite broad as it refers to providing any assistance\(^2\) 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 there under shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

\(^1\) All systems connected to the Internet can be affect by denial-of-service attacks. Intruders can flood networks with overwhelming amounts of traffic or cause machines to crash or otherwise become unstable. Such attacks block the authorized users from using the site services. EBay, Amazon, CNN, Yahoo! have faced distributed denial-of-service (DDoS) attacks in the recent past.

\(^2\) The words ‘any assistance’ in section 43(g) are very wide to include any acts or omissions which have a direct nexus with or which can be related to any facilitation unauthorized access to any computer, computer system or computer network, in contravention of the provisions of the Indian Cyber law.
It is important to note that the definition of access [Sec. 2(1)(a)] which provides for gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network, very well articulates technological aspects of access.

Sec. 43 (h): Unauthorized Charge

The advent of personal computers and the merger of computer and communications technology have created a vast market of computer services. An unimaginable amount of electronic data is now available for a fee from a wide array of commercial services. Hence computer services may also be the subject of the offence of theft of services. While unauthorized access typically is intended to protect networks operated by individuals and businesses, theft of services statutes by unauthorized charge is additionally intended to protect Internet Service Provider (ISP). Sec. 43(h) provides for making a person liable who, “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”. A technique that has become infamous for such acts is the salami attack where a cyber thief will steal thousands at once, using each card only a single time so that the crime has a higher chance of going unreported. These types of activities have been dubbed “salami” attacks because the perpetrator is shaving off an imperceptibly small piece of the larger asset.

5.1.2 Sec. 43 A- 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. (Change vide ITAA 2008)

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 unauthorized 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.

In view of recent concerns about handling sensitive personal data in the BPO sector, sub-section A is being added in section 43 [Section 43 A]¹ of the IT Act to provide damages against corporate bodies, handling sensitive personal data, in case they are found to be negligent in implementing and maintaining reasonable security practices and procedures, it shall be liable to pay by way of compensation not exceeding rupees one crore to the person affected. The changes will increase pressure on the business process outsourcing (BPO) companies.

5.1.3. Penalty for failure to furnish information return:

Sec. 44 provides penalties for, a failure to furnish or file any information or maintain a books of account, which are specified under the ITA or any rules or regulations made there under.²

¹ Section 43 A Inserted vide Information Technology (Amendment) Act, 2008
² Section 44- If any person who is required under this Act or any rules or regulations made there under to-
(a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
(b) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;
(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.
It is important to note that the sec. 44 imposes a range of penalties on any person who is required under this Act or any rules or regulations made there under. Sec. 44(a) prescribes a penalty not exceeding one lakh and fifty thousand rupees for each such failure to furnish any document, return or report to the Controller or the Certifying Authority (CCA). Sec. 44(b) prescribes a penalty not exceeding five thousand rupees for every day during which a failure continues with respect to filing any return or furnishing any information, books or other documents within the time specified there in the regulations or failure to file return or furnish the same within the time specified there in the regulations. Sec. 44(c) prescribes a penalty not exceeding ten thousand rupees for everyday during which a failure continues to make or maintain books of account or records.

The category of “any person” includes any company or association or individual or body of individuals, whether incorporated or not, or local authority, government organization/agency, etc.

5.1.4. Residuary Penalty

Sec. 45 provides for a residuary penalty for the IT Act or any rules or regulations there under.\(^1\) The section is attracted when there is a contravention of provisions of the IT Act or any rules or regulations and no penalty has been specifically provided for the contravention (Sec.43 and 44). The section provides for the payment of penalty for such contravention or compensation to the person who has been affected by such a contravention for a sum not exceeding twenty-five thousand rupees.\(^2\)

In the interpretation of statutes, the courts always presume that the legislature inserted every part thereof for a purpose and the legislature intention is that every part of the statute should have an effect.\(^3\)

---

1. 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


5.1.5. Compounding of Contraventions

Section 63 provides for compounding of contravention (Sec.43-45) under the Act. Compounding of 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". Compoundable offence is an offence which is capable of being compounded or which the law allows to be compounded privately between the parties. Sub-section (1) of section 63 permits compounding of contravention (Sec.43-45). Such compounding can be before as well as after the institution of adjudication proceedings. Therefore, during the stage of the adjudication proceedings, compounding of the alleged contravention is permitted. The Controller is empowered to compound the contravention. He can also authorize a particular office especially for this purpose. Apart from the Controller or the officer authorized by him, even the adjudicating officer has the power to compound offences. Conditions can be laid down by the Controller or such authorized officer or the adjudicating officer while compounding the offence. However, the proviso to sub-section (1) of section 63 provides that the sum shall not exceed the maximum amount of the penalty which may be imposed under the Act for the contravention so compounded. Sub-section (3) prohibits any proceedings to be started against the person guilty of such contravention in respect of the contravention so compounded.

Section 63(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 authorized 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 purpose 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.

initiated or any proceeding already initiated to be further progressed against a person guilty of a contravention which has been compounded.\textsuperscript{1}

Surprisingly, compounding of contraventions under the sub-section (1) does not include the ‘complainant’ or the person so affected by such contraventions. Further, as in Rule 11 of the Information Technology Rules, 2003, the contravener may make an application for compounding the contravention during the adjudicating proceedings to be concerned Adjudicating Officer.\textsuperscript{2} The Act, however, does not prescribe any circumstance or situation under which compounding of contravention can take place.

Sub-section (2) acts as an exception of sub-section(1) to the effect that it states situation where compounding would not be permitted. If a person commits the same or similar contravention within a period of three years from the date on which the first contravention was committed by him, then the benefit of compounding of contravention under sub-section (1) would not be available to the person contravening. However, the Explanation clarifies that for the purpose of sub-section (2), 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. Effectively, that would mean that the option of compounding of contravention would be available in case the same or similar contravention has been made after a lapse of three years.

It should, however, be noted that section 63 provides only for compounding of contraventions (enumerated in chapter IX) and not compounding of offences (under chapter XI). Reading section 63 with section 45 (residuary clause), contravention under the rules and regulations made under the Act is also compendable.

5.1.6. Recovery of Penalty

The penalty amount on account of contraventions as under section 43, 44 and 45 whether compounded must not exceed one crore of rupees. Section 64

provides that when, “a penalty imposed under the IT Act, is not paid, then it shall be recovered as an arrear of land revenue and the licence or the Electronic Signature Certificate,¹ as the case may be, shall be suspended till the penalty is paid”. However, if the person is neither a Certifying Authority nor a subscriber of an Electronic Signature Certificate, then in that case recovery of penalty is restricted to an arrear of land revenue only.

It is interesting to note that land revenue is a state subject under List II in the Seventh Schedule to the constitution. Different states have enacted their respective land reforms and land revenue Acts, Rules and Regulations for the purposes of collecting land revenue and the recovery of its arrears. That is, recovery of penalty under sec. 64 of the Act will follow the state’s enactment and collected accordingly, till the time state Government may make separate rules for this purpose under sec. 90 of the Act.

5.1.7. Surrender of Licence

Under the Section 33(1) every Certifying Authority whose licence has been suspended or revoked² is to surrender its licence to the controller immediately.

Any such failure on the part of the person to comply with the directions as given in sub-section (1) is to be taken as a non-cognizable and bailable offence.

¹ Amended vide Information Technology (Amendment ) Act, 2006
² Sec. 25 Suspension of licence-
(1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has—
   a. made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;
   b. failed to comply with the terms and conditions subject to which the licence was granted;
   c. failed to maintain the standards specified under clause (b) of sub-section (2) of section 20;
   d. contravened any provisions of this Act, rule, regulation or order made thereunder, revoke the licence;
Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.
(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1), by order suspend such licence pending the completion of any inquiry ordered by him:
Provided that no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.
(3) No Certifying Authority whose licence has been suspended shall issue any Digital Signature Certificate during such suspension.
The said person is to be punished with imprisonment, which may extend up to six months or a fine, which may extend up to ten thousand rupees or with both.

One should not miss the importance that has been given to this aforesaid section in the Act. It indicates seriousness on the part of the legislature to make non-submission of a suspended or revoked licence an offence rather than a contravention under the Act.

5.2. Offences under the IT Act

A contravention is a mere violation of law or rule of procedure. It may or may not be punishable with a liability to pay a penalty (or compensation) only. An offence is an act prohibited and made punishable by fine and/or imprisonment. Contravention is generic whereas offence is specific.

The difference between ‘cyber contravention’ and ‘cyber offence’ is more about the degree and extent of criminal activity rather than anything else. For example, a mere unauthorized access to a computer, computer system or computer network may amount to ‘cyber contravention’ but for a ‘cyber offence’ it is the specific criminal violation that resulted from the unauthorized access to a computer, computer system or computer network that has to be taken into consideration.

There exists a thin line of demarcation between cyber contraventions and cyber offences. For example, one can observe on a closer reading of S. 43(a) to (h) and S.66 of the Act that there exists very little difference between the provisions of S. 43 and S.66 of the Act. While the former is about ‘cyber contravention’, the latter is about ‘cyber offence’. Surprisingly, both sections refer about unauthorized access, modification, damage, disruption of any computer, computer system or computer network.

The judicial authority may have to carefully examine the facts and circumstances of each case before pronouncing their judgments, taking cognizance of either S. 43 of S. 66 of the Act. In case of a difficulty, it would be prudent to look into the legislative intent behind the construction of these two sections. Similarly, it is important that both cyber contraventions and cyber offences under
the Act must be classified accordingly and distinguished from one another for proper understanding and application.

<table>
<thead>
<tr>
<th><strong>Cyber Contraventions under the Act</strong></th>
<th><strong>Cyber Offences under the Act</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Deals primarily with unauthorized access to computer, computer system or computer network</td>
<td>Deals with computer, computer system or computer network related serious offences</td>
</tr>
<tr>
<td>S.43(a)to(h)</td>
<td>Ss. 65-74</td>
</tr>
<tr>
<td>May result in civil prosecution</td>
<td>May result in criminal prosecution</td>
</tr>
<tr>
<td>Judicial proceedings before the Adjudicating Officer</td>
<td>Judicial proceedings to be held before the appropriate 'Court' as per the nature of offence, whether cognizable or non-cognizable</td>
</tr>
<tr>
<td>Provisions of the Limitation Act, 1963 apply to an appeal made to the Cyber Appellate Tribunal</td>
<td>Period of limitation for taking cognizance of certain offences shall be as specified in Sections 468- 473 of the Cr.P.C.</td>
</tr>
<tr>
<td>Compounding of contraventions</td>
<td>No compounding of offences</td>
</tr>
<tr>
<td>Power to investigate any contravention lies with the Controller or any officer authorized by him</td>
<td>Power to investigate any offence lies with the police officer not below the rank of Inspector</td>
</tr>
<tr>
<td>Offender liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.</td>
<td>Offender punishable with imprisonment term or fine or with both</td>
</tr>
</tbody>
</table>
The First Schedule of the Code of Criminal Procedure, 1973 provides *inter alia* the Classification of Offences (I-Offences under the Indian Penal Code, and II-Classification of offences against other laws). The table below shows the classification of offences against other laws:

<table>
<thead>
<tr>
<th>Offence</th>
<th>Cognizable(^1) or Non-cognizable(^2)</th>
<th>Bailable or Non-bailable(^3)</th>
<th>By what Court triable</th>
</tr>
</thead>
<tbody>
<tr>
<td>If punishable with death, imprisonment for life, or imprisonment for more than 7 years</td>
<td>Cognizable</td>
<td>Non-bailable</td>
<td>Court of Session</td>
</tr>
<tr>
<td>If punishable with imprisonment for 3 years and upwards but not more than 7 years</td>
<td>Cognizable</td>
<td>Non-bailable</td>
<td>Magistrate of the first class</td>
</tr>
<tr>
<td>If punishable with imprisonment for less than 3 years or with fine only</td>
<td>Non-cognizable</td>
<td>Bailable</td>
<td>Any Magistrate</td>
</tr>
</tbody>
</table>

1. S. 2(c) of Cr. P.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 any other law for time being in force, arrest without warrant.
2. S. 2(1) of Cr. P.C. "non-cognizable offence" means an offence for which, and "non-cognizable case" means a case in which, a police officer has no authority to arrest without warrant.
3. S. 2(a) of Cr. P.C. "bailable offence" means an offence which is shown as bailable in the First Schedule, or which is made bailable by any other law for time being in force; and "non-bailable offence" means any other offence.
Chapter XI of the IT Act, 2000 has been classified as cognizable/non-cognizable, bailable/non-bailable and by what Court triable in the table below:

<table>
<thead>
<tr>
<th>Section</th>
<th>Offence</th>
<th>Cognizable/Non-cognizable</th>
<th>Bailable/Non-bailable</th>
<th>By what Court triable ?</th>
</tr>
</thead>
<tbody>
<tr>
<td>S. 65</td>
<td>Tampering with computer source documents</td>
<td>Cognizable</td>
<td>Non-bailable</td>
<td>Magistrate of the first class</td>
</tr>
<tr>
<td>S.66</td>
<td>Hacking with computer system</td>
<td>Cognizable</td>
<td>Non-bailable</td>
<td>Magistrate of the first class</td>
</tr>
<tr>
<td>S.67</td>
<td>Publishing of information which is obscene in electronic form</td>
<td>Cognizable</td>
<td>Non-bailable</td>
<td>Magistrate of first class</td>
</tr>
<tr>
<td></td>
<td>First Conviction</td>
<td>Cognizable</td>
<td>Non-bailable</td>
<td>Court of Session</td>
</tr>
<tr>
<td></td>
<td>Second Conviction</td>
<td>Cognizable</td>
<td>Non-bailable</td>
<td></td>
</tr>
<tr>
<td>S.68</td>
<td>Power of the Controller to give directions</td>
<td>Cognizable</td>
<td>Non-bailable</td>
<td>Magistrate of the first class</td>
</tr>
<tr>
<td>S.69</td>
<td>Directions of Controller to a subscriber to extend facilities to decrypt</td>
<td>Cognizable</td>
<td>Non-bailable</td>
<td>Magistrate of the first class</td>
</tr>
<tr>
<td>S.70</td>
<td>Protected system</td>
<td>Cognizable</td>
<td>Non-bailable</td>
<td>Court of Session</td>
</tr>
<tr>
<td>S.71</td>
<td>Penalty for misrepresentation</td>
<td>Non-Cognizable</td>
<td>Bailable</td>
<td>Any Magistrate</td>
</tr>
<tr>
<td>S.72</td>
<td>Breach of confidentiality and privacy</td>
<td>Non-Cognizable</td>
<td>Bailable</td>
<td>Any Magistrate</td>
</tr>
<tr>
<td>S.73</td>
<td>Penalty for publishing Digital Signature Certificate false in certain particulars</td>
<td>Non-Cognizable</td>
<td>Bailable</td>
<td>Any Magistrate</td>
</tr>
<tr>
<td>S.74</td>
<td>Publication for fraudulent purpose</td>
<td>Non-Cognizable</td>
<td>Bailable</td>
<td>Any Magistrate</td>
</tr>
<tr>
<td>S. 33</td>
<td>Surrender of licence</td>
<td>Non-Cognizable</td>
<td>Bailable</td>
<td>Any Magistrate</td>
</tr>
</tbody>
</table>

Classification of offences under the Information Technology (Amendment) Act, 2008:-

“S-77B Offences with three years imprisonment to be cognizable

(1) Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable”.

The operation 1st Schedule of the Cr. P.C. has been made inapplicable by insertion of this section. However, with the insertion of this section, the offences can be categorized as under:

<table>
<thead>
<tr>
<th>OFFENCE</th>
<th>Cognizable or non cognizable</th>
<th>Bailable or Non-bailable</th>
</tr>
</thead>
<tbody>
<tr>
<td>The offence punishable with imprisonment less than 3 years</td>
<td>Non cognizable</td>
<td>Bailable</td>
</tr>
<tr>
<td>The offence punishable with imprisonment of three years</td>
<td>Cognizable</td>
<td>Bailable</td>
</tr>
<tr>
<td>The offence punishable with imprisonment of more than three years</td>
<td>Cognizable</td>
<td>Non-Bailable</td>
</tr>
</tbody>
</table>

Thus, as per the scheme of the newly inserted Section 77-B, the offences under the amendment Act can be classified as follows:

<table>
<thead>
<tr>
<th>Offence</th>
<th>Punishment</th>
<th>Cognizable or non cognizable</th>
<th>Bailable or Non-bailable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 65: Tampering with computer source documents</td>
<td>Imprisonment upto three years and/or Fine upto Rs. 2 Lakhs</td>
<td>Cognizable</td>
<td>Bailable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Offence</th>
<th>Punishment</th>
<th>Cognizable or non cognizable</th>
<th>Bailable or Non-bailable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 66 : Hacking with Computer system (if done dishonestly or fraudulently)</td>
<td>Imprisonment upto three years and/or Fine upto Rs. 5 Lakhs</td>
<td>do</td>
<td>do</td>
</tr>
<tr>
<td>Section 66 A: Punishment for sending offensive messages through communication service, etc</td>
<td>Imprisonment for a term which may extend to three years and with fine</td>
<td>do</td>
<td>do</td>
</tr>
<tr>
<td>Section 66 B: Punishment for dishonestly receiving stolen computer resource or communication device</td>
<td>Imprisonment upto three years and/or Fine upto Rs. 1 Lakhs</td>
<td>do</td>
<td>do</td>
</tr>
<tr>
<td>Section 66 C: Punishment for identity theft</td>
<td>Imprisonment upto three years and Fine upto Rs. 1 Lakhs</td>
<td>do</td>
<td>do</td>
</tr>
<tr>
<td>Section 66 D: Punishment for cheating by personation by using computer resource</td>
<td>-do-</td>
<td>-do</td>
<td>-do</td>
</tr>
<tr>
<td>Section 66 E: Punishment for violation of privacy</td>
<td>Imprisonment upto three years and/or Fine upto Rs. 2 Lakhs</td>
<td>do</td>
<td>do</td>
</tr>
<tr>
<td>Section 66 F: Punishment for cyber terrorism</td>
<td>May extend to Life imprisonment</td>
<td>do</td>
<td>Non-bailable</td>
</tr>
<tr>
<td>Section 67 : Publishing obscene information in electronic form</td>
<td><strong>First Conviction:</strong> Imprisonment upto three years and Fine upto Rs. 5 Lakhs</td>
<td>do</td>
<td>Bailable in case of first conviction only. Second or subsequent conviction shall be non bailable</td>
</tr>
<tr>
<td></td>
<td><strong>Second or subsequent Conviction:</strong> Imprisonment upto five years and Fine upto Rs. 10 Lakhs</td>
<td>do</td>
<td></td>
</tr>
<tr>
<td>Section 67 A: Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form</td>
<td><strong>First Conviction:</strong> Imprisonment upto Five years and Fine upto Rs. 10 Lakhs</td>
<td>-do</td>
<td>Non-bailable in both first and second conviction</td>
</tr>
<tr>
<td>Offence</td>
<td>Punishment</td>
<td>Cognizable or non cognizable</td>
<td>Bailable or non-bailable</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Section 67B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form</td>
<td>-do-</td>
<td>-do-</td>
<td>-do-</td>
</tr>
<tr>
<td>Section 67C(2): Deliberate Failure by the intermediary to preserve and retain information as specified by the Central Government</td>
<td>Imprisonment upto three years and Fine</td>
<td>-do-</td>
<td>Bailable</td>
</tr>
<tr>
<td>Section 68(2): Deliberate Failure to comply with the order/direction of controller</td>
<td>Imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both</td>
<td>Non cognizable</td>
<td>-do-</td>
</tr>
<tr>
<td>Section 69 (1): Failure to extend facilities to decrypt information to govt. notified agency</td>
<td>Imprisonment for a term which may extend to seven years and fine</td>
<td>Cognizable</td>
<td>Non-bailable</td>
</tr>
<tr>
<td>Section 69A(3): Punishment for failure by the intermediary to comply with the order of the notified agency to block websites etc.</td>
<td>-do-</td>
<td>-do-</td>
<td>-do-</td>
</tr>
<tr>
<td>Section 69B (4): Deliberate failure by the intermediary to provide the notified agency with the technical assistance or online access to the computer resource</td>
<td>Imprisonment for a term which may extend to three years and fine</td>
<td>Non Cognizable</td>
<td>Bailable</td>
</tr>
<tr>
<td>Section 70: Unauthorized access to protected system directly or indirectly affects the facility of Critical Information Infrastructure</td>
<td>Imprisonment up to 10 years and fine</td>
<td>Cognizable</td>
<td>Non-bailable</td>
</tr>
<tr>
<td>Section 72A: Punishment for disclosure of information in breach of lawful contract</td>
<td>Imprisonment for a term upto three years or to a fine upto Rs. 5 Lakhs or to both</td>
<td>-do-</td>
<td>Bailable</td>
</tr>
</tbody>
</table>
5.2.1. Tampering with Computer Source Documents

The offence of tampering with computer source documents under section 65 is made out when a person:

(i) intentionally conceals, destroys or alters a computer source code used for a computer, computer programme, computer system or computer networks;

(ii) intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network; and

(iii) (a) the offence is made out only when computer source code is required to be kept or
(b) when computer source code is maintained by law for the time being in force.

What is a "Computer Source Code" is also defined in the Explanation to section 65 of the Act. By the very definition of 'computer source code', (a) list of programmes; (b) computer commands; (c) design and layout and (d) programme analysis of computer resources in any form, is a 'computer source code' for the purpose of section 65 of the IT Act.1

It is to be noted that when computer source code is not required by law to be kept or maintained then tempering with computer source code is not punishable and that is not proper.2 Furthermore, it is important to know that the Act makes no mention whether the source code exists in tangible (on paper) or intangible (electrical impulses) form. The Act accepts the computer source code in both

---

1 Section 65-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.


tangible and intangible form. Importantly, by virtue of the Explanation, the term 'computer source code' also includes the software program's 'object code' as well.

The idea behind the section 65 is to protect the 'intellectual property' invested in the computer programmes. It is an attempt to extend the protection to computer source documents (codes) beyond what is available under copyright laws.¹

The word 'knowingly' or 'intentionally', 'conceal', 'alter' has not been defined under the I.T. Act.

The section proposes punishment with imprisonment up to three years, or with fine, which may extend up to two lakh rupees, or with both. It could be argued that the fine amount has been kept so infinitesimally low that it would in no way ever compensate the victim's electronic losses in real terms. Nevertheless, the offence under the section has been made both cognizable and non-bailable.

5.2.2 Hacking with Computer system

Before I.T. (Amendment) Act, 2008:- Hacking has been very widely defined in the law of Information Technology, which is much wider than the concept of "hacking" as understood in common parlance, i.e. breaking into computer systems.²

Section 66 makes it an offence to hack with a computer system.³ For the offence to be committed, certain requisites have to be satisfied, these are, either the mens rea-

---

³ Section 66- (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. (2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

*The I.T. (Amendment) Act, 2008 amended Section 66. This amended provision applies to only of the act is done "dishonestly" or "fraudulently". New Sections added under 66A, 66B, 66C, 66D, 66E and 66F to cover new offences.
(a) the intent to cause loss or damage; or
(b) the knowledge that the actions are likely to cause wrongful loss or damage to the public or any person, or either the actus reus:
(i) destroys, delete, or alter any information;
(ii) diminish the value or utility of any information; or
(iii) affect injuriously by any means any information residing in a computer resource.

The section is an amend form of section 425 of the IPC, 1860, with the word, with the term, "property" being replaced in the section with, "information residing in a computer resource".

An intent to cause damage may be ascertained, when, "it exists in idea before it exists in fact, the idea realizing itself in the fact because of the desire by which it is accompanied". Knowledge may be defined as an awareness or understanding of a fact or circumstance. The term "wrongful loss", finds definition under section 23 of the IPC, 1860, as "the loss by unlawful means of property to which the person losing it is illegally entitled.... 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". Hence, unless the information contained in the computer resource was destroyed or altered due to the action of the accused so that its utility or value was diminished, no offence under section 66 of the Act could be said to have been committed. Requiring proof of knowledge or at last reason to know places some burden on the system owner to communicate restrictions on use to other parties, but avoids placing criminal liability on an individual's for what may in fact be entirely bona fide actions. Moreover, most acts of, "hacking requires expertise, forethought and planning", thus having in them an inherent, criminal intent or knowledge.

It is important to point out that, intention and knowledge are distinct. There may be intention without knowledge, the consequence being desired but not, certain or even probable. Conversely, there may be knowledge without intention, the consequence being inevitable concomitant of that which is desired, but being itself an object of repugnance rather than desire, and therefore unintended.

The section also requires that, the hacker must destroy, delete, or alter any information, residing in any computer resource. A differentiation is made between the acts of, destruction and deletion though in practice they are used interchangeably. Deletion is on a lower threshold, than destruction. When a user, 'deletes' a file, the computer performs the following functions, (a) the file becomes invisible to the operating system; and (b) the space occupied by the file in freed up for use, allowing the operating system to overwrite that space with new information. Unless the operating system requires use of this space, overwriting does not occur and "deleted" data remains for a considerable time.1 "Deletion" of data is the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognizable.2 Deletion may lead the data to be recoverable whereas destruction implies that the data is irretrievable.

Diminishing of the value or utility of information also constitutes the crime of hacking under section 66. Though what actions constitute, the diminishing the value or utility of information residing in a computer resource, is not explained throughout the I.T. Act. Another form of hacking, "causing injury to information" is similarly not defined throughout the I.T. Act, 2000.

Section 43 and 66 of the Act

Sec. 43 of the I.T. Act provides for damages by way of compensation not exceeding rupees one crore to the person so affected, on the commission of either or more of the following acts done by any person without the permission of the


owner or any other person who is in-charge of a computer, computer system or computer network.

- Access to such computer, computer system or computer network.  
  \[1\]
- Damage to any computer, computer system or computer network, data, computer data base or any other programme residing in such computer, computer system or computer network.  
  \[2\]
- Disruption of any computer, computer system or computer network.  
  \[3\]
- Assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the I.T. Act, rules or regulations made there under.  
  \[4\]

The aforesaid acts can also be committed by "hacking" as the expression is used in common parlance, i.e. breaking into computer system.  

As it has been argued earlier that there exist a thin line of demarcation between the provision of section 43 and section 66 of the Act. The question is now to distinguish whether a cyber crime falls under section 43 or section 66 of the Act. For a cyber crime to fall under section 66, one must observe whether criminal intent was present or not. Criminal intention simply means the purpose or design of doing an act forbidden by the criminal law without just cause or excuse. An act is intentional if it exists in idea before it exists in fact, the idea realizing itself in the fact because of the desire by which it is accompanied. The criminal intent in hacking manifests itself in terms of causing wrongful loss or damage, destroying or altering any information residing in a computer source or diminishing its value or utility or affects it injuriously by any means.

For example, a person causing a computer virus to enter into circulation is intentionally trying to impair the operation of a computer or any program or data. The originator (or any other party who deliberately causes the dissemination of the virus) will be held responsible for the modification (impairment) of any computer,

---

1 Section 43(a) of the IT Act, 2000
2 Section 43(d) of the IT Act, 2000
3 Section 43 (e) of the IT Act, 2000
4 Section 43 (g) of the IT Act, 2000
which is infected even though he may not be responsible for the infection of any particular machine. Prima facie, the said person could reasonably be tried under section 43(c) or section 66 of the Act. Hence, in order to distinguish applicability of the sections, one may have to look into the circumstances and accompanying events to reconstruct the 'chain of events' leading to circulation of computer virus. If the 'chain of events' points out a premeditated, well-planned activity then it underlines the presence of criminal intent to cause wrongful loss or damage and the section applicable would be section 66 of the Act. Any absence of 'criminal intent' would still make it punishable under section 43(c) of the Act.¹

After IT (Amendment) Act, 2008

Section 66J Computer Related Offences (Substituted vide ITAA 2008): If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Explanation: For the purpose of this section,-

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

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

Section 66 A] Punishment for sending offensive messages through communication service, etc.( Introduced vide ITAA 2008): 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,

(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 (Inserted vide ITAA 2008).

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.

[Section 66 B] Punishment for dishonestly receiving stolen computer resource or communication device (Inserted Vide ITA 2008): Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

[Section 66C] Punishment for identity theft. (Inserted Vide ITA 2008): Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

[Section 66D] Punishment for cheating by personation by using computer resource (Inserted Vide ITA 2008): Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

[Section 66E] Punishment for violation of privacy. (Inserted Vide ITA 2008):

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.

|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 authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70. or
(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

5.2.3. Publishing or transmitting obscene material in electronic form

Section 67 prohibits publication or transmits of information that is obscene in electronic form. The ingredients of Section 67 are:-

(a) publication or transmission in the electronic form
(b) material lascivious or appeals to the prurient interest
(c) tendency to deprave and corrupt persons
(d) likely – audience
(e) to read, see or hear the matter contained or embodied in electronic form.

1 Amended vide Information Technology (Amendment) Act, 2008.
2 Section 67- 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 effects in 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.
The word 'publication' has not been defined under the Act. Thus, as discussed above, publication or transmission in the electronic form includes dissemination, storage and transmission of information or data in electronic form. And in order to comprehend the meaning of "electronic form" as defined under section 2(1)(r) properly, due credence should also be given to the definitions, like "information" (section 2(1)(v)) and "data" (section 2(1)(o)).

The section advocates that the "obscene material in electronic form" must be considered by itself and separately to find out whether it is so gross and its obscenity 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 'obscene material in electronic form' is likely to fall.

An important thing to note is that though publication or transmission of obscene material in an electronic form is an offence but merely browsing or surfing obscene material on the internet or possessing such material in the privacy of one's home is not an offence. It is only, when the material is disseminated, published or transmitted in an electronic form; it becomes an offence under section 67. In other words, transmission and not mere possession of obscene information is an offence and therefore, section 67 does cover within its ambit pornographic websites, pornographic magazines produced using computers as well as transmitting pornographic pictures, photos, writings etc through the internet. In case where the obscene materials are in the form of video, the persons who have acted in the video, the persons who have shot the video and every person in the chain of distribution is covered within the ambit of the section.

---

1 "electronic form" with reference to information means any information generated, sent received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.
2 "information" includes data, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche.
3 'data' means 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, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.
The fact that transmission was addressed to an intended person for his personal use is immaterial. The act of transmission alone is sufficient to label an act as an offence if the essentials laid down in section 67 are found to exist. The plea that the audience of the transmission was desired to be the selected people is unsustainable if others are likely to have access to it. Even a single transmission makes the person publisher and thus liable to be prosecuted and punished under the section if material is lascivious or appeal to the prurient interest of the people.

Section 67 of the I.T. Act defines an offence substantially similar to section 292 IPC. Critically speaking, section 292 (1) of IPC\(^1\), does not make

---

\(^1\) Section 292-(1) For the purposes of sub-section (2) book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene, if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items the effect of any one of its items) is, if taken as a whole, such as to tend to deprave and corrupt 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 possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object what so ever, or

(b) imports, exports or conveys any obscene object for any of the purposes aforesaid, or knowing or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation, or

(c) takes part in or receives profits from any business in the course of which he knows or has reason to believe that any such obscene objects are, for any of the purposes aforesaid, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation, or

(d) advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be procured from or through any person, or

(e) offers or attempts to do any act which is an offence under this section, shall be punished on first conviction with imprisonment of either description for a term which may extend to two years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees.

Exception- This section does not extend to-

(a) any book, pamphlet, paper, writing, drawing, 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 (24 of 1958), or

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

---

315
knowledge of obscenity an ingredient of the offence. Thus to escape criminal charges, one has to prove his lack of knowledge of publication or transmission of obscene information in electronic form. Moreover, though publication or transmission of obscene information may be illegal but mere possession, browsing or surfing through obscene content is not an illegal activity. Another missing link in the section 292, IPC, i.e., the exceptions which are available on account of public good, religious purposes, etc. may not be available if such publication or its transmission is in the electronic form. It should be noted that under no circumstances any offence related to 'obscenity in electronic form' should be tried under section 292, IPC as section 81 of the I.T. Act, 2000 states that the Act will have an overriding effect:

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

**Difference between Section 67 of the I.T. Act, 2000 and Section 292 of the IPC, 1860:-**

1. The punishment under section 67 is much more stringent than that under section 292. Under section 67 on first conviction the punishment is imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to ten lakh rupees. However, under section 292 the punishment 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.
2. According to the Code of Criminal Procedure, 1973 the offence under section 67 of the I.T. Act is cognizable and non-bailable whereas the offence under section 292 of the IPC, 1860 is cognizable and bailable.

3. On first conviction, the offence under section 67 is triable by Magistrate of the first class and on second conviction it is triable by the court of session whereas the offence under section 292 of the IPC is triable by any Magistrate.

4. Section 67 of the I.T. Act, 2000 does not expressly contain any of the exceptions enlisted in Section 292 of the IPC, 1860.

Neither the I.T. Act, 2000 nor the IPC gives any meaning to the terms "lascivious" or "prurient". Neither are there any uniform standards for determining what is lascivious or prurient nor there can be. 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.

The judiciary has adopted the, "Heckling test", 1 enunciated by, Justice Cockburn, to determine what constitutes, 'obscenity'.2 The Supreme Court has held that, the test of obscenity is, whether the, "tendency of the matter charged as obscene is to deprave and corrupt those whose minds are open to such immoral influences." It has been held that the test of obscenity to adopt in India is that obscenity, without a preponderant social purpose or profit. Obscenity in such cases cannot have the constitutional protection of free speech.3

The IT (Amendment) Act, 2008 amended section 67 and introduced new section 67A, 67B and 67C.

1. (1863) 3 QB 360, 371.
[Section 67] Punishment for publishing or transmitting obscene material in electronic form (Amended vide ITAA 2008): Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

[Section 67 A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form (Inserted vide ITAA 2008): Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

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

(ii) which is kept or used bona fide for religious purposes.
[Section 67 B] Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form: Whoever,-

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

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

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

(d) facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

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

(ii) which is kept or used for bonafide heritage or religious purposes

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.
[Section 67 C] Preservation and Retention of information by intermediaries:

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

5.2.4 Power of controller to give directions

Section 68 gives additional powers to the controller to give various directions to ensure compliance with the provisions of the I.T. Act, 2000, rules and regulations made there under.1 Though it is very much evident from the wordings of the sec. 68 that the Controller could only give directions to a Certifying Authority or any employee of such Authority, but the fact is that his power may also be extendable to the subscriber of a digital signature certificate, by virtue of sec. 18 (1), which states that the Controller has also the power to resolve any conflict of interests between the Certifying Authorities and the subscribers.

Any persons who fails to comply with any order under sections 68(1), shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both. That is, the offence under the section 68 is cognizable and non-bailable one.

Further more, power under section 68 can also be exercised by Deputy Controller, Assistant Controller or any other officer to whom such

1 Section 68-(1) The Controller may, by order, direct a Certifying Authority or any employee 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 the this Act, rules or any regulations made there under.

(2) Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

*The I.T. (Amendment) Act, 2008 amended section 68(2), the word intentionally or knowingly is being added to include and reducing penalty not exceeding two years or to a fine not exceeding one lakh rupees or to both.
powers have been delegated by the Controller by virtue of his power under section 271

In this way Controller is vested with ample power so as to ensure compliance of the provisions of the Act. The legislators anticipated that in absence of strong enforcement machinery the Act will become a paper tiger and will not be successful in achieving its aims and objectives.

The IT (Amendment) Act, 2008 amended section 68.

[Section 68] Power of Controller to give directions (Amended Vide ITAA 2008):

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

(2) Any person who intentionally or knowingly (Inserted vide ITAA 2008) 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.

5.2.5 Directions of Controller to a subscriber to extend facilities to decrypt information

Section 69(1)2 makes the Controller, the sole statutory authority under the Act to direct any agency of the Government to intercept any information transmitted through any computer resource, which includes computer, computer system, computer network, data, computer database or software [Sec.2 (1) (k)].

1 Section 27-The Controller may, in writing, authorize the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

2 Section 69-(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.
Certain prerequisites must be fulfilled to the satisfaction of the controller before an order for interception may be made under section 69(1), these include, (a) interest of the sovereignty or integrity of India, (b) the security of the state, (c) friendly relations with foreign states, (d) public order, (e) preventing incitement to the commission of any cognizable offence. The section also provides that the reasons for the interception should be recorded in writing.

Our may argue that the section 69 of the Act is violative of the Article 19(1) (a) and Article 21 of the Constitution. The former grants "right to freedom of speech and expression", whereas the latter is about "right to privacy".

When a person is sending or receiving electronic communication through any computer resource, he is exercising his right to freedom of speech and expression, enumerated under Article 19 (1) (a) of the Constitution. Electronic communication tapping, unless it comes within the grounds of reasonable restrictions imposed by the state relating to defamation, contempt of court, decency or morality, morality of the state, friendly relations with foreign states, incitement to an offence, public order, maintenance of the sovereignty and integrity of India under Article 19 (2), would infract Article 19(1)(a) of the Constitution.

Similarly, the right to send or receive electronic communication's in the privacy of one's home or office without interference can certainly be claimed as a "right to privacy", which is a part of the right to "life and personal liberty". Any attempt to intercept electronic communication would interact Article 21 of the Constitution unless it is permitted under the procedure established by law.

Under section 69 of the I.T. Act, similar grounds of reasonable restrictions have been cited for enabling the controller to direct interception of any information transmitted through any computer resource. Section 69 of the I.T. Act, 2000 does not use the word "reasonable restriction". However,
it does enable the grounds of reasonable restrictions to be the grounds on which the Controller can order interception decryption of any information transmitted through any computer resource.

It can be argued that section 69 of the I.T. Act, 2000 infracts the fundamental rights 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. 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) 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.

In fact, a perusal of the new cyber law and the rules and regulations made there under show that there is no specific power granted there under for the framing of rules under section 69 of the I.T. Act, 2000. In fact, the formulation of any rules, procedural or otherwise. In the absence of just and fair procedure for regulating the exercise of power under section 69, it may not be possible to safeguard the rights of the citizens guaranteed under Articles 19 (1) (a) and 21 of the Constitution of India. As such, it would be prudent for the controller to abide, as far as possible, by the spirit of the aforesaid guidelines issued by the Supreme Court while directing interception of information transmitted through any computer resource.

Section 69 (2) directs the subscriber, i.e., a person in whose name the digital signature certificate is issued by a licensed certifying authority or any person in-charge of the computer resource, to extend all facilities and technical assistance to decrypt the information, as and when called upon by any agency,

---

1 Section 69 (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.
which has been directed by the Controller under the circumstances as prescribed under sub-section (1).

It is important that the meaning of 'decryption' should be understood in terms of encryption/decryption mechanism of a key pair.

The failure of the subscriber or any person to assist the agency in extending all facilities and technical assistance to decrypt the information has been made a penal offence punishable with imprisonment, which may extend to seven years (Section 69 (3)).

Section 69 (2) uses the words "the subscriber shall extend all facilities and technical assistance to decrypt the information." It may be possible that the subscriber or any person in-charge of the computer resource may not have all or any facility or technical assistance to decrypt the information as every subscriber has not facilities and technical assistance for decryption.

In the light of this scenario, and also in view of 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. It is fair to punish someone for failing to assist the intercepting agency on the ground of not extending all 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 intercepting agency, due to their economic inability or for not providing a facility that he does not have or that he cannot afford. It is incumbent upon the intercepting agency to take resource to all technical assistance and facilities on its own for the purpose of decryption.

Encryption as a subject has not been dealt with under the I.T. Act, 2000. The relevant question that comes up for consideration is whether encryption is permissible under the I.T. Act, 2000? It is clear that there is no specific bar under I.T. Act on encryption. Since the law does not bar encryption, a logical interpretation would be that it is permissible, but the subject has not been specifically elucidated under the I.T. Act, 2000. Also, since the law talks of decryption, it presumes the existence of encryption at
the first instance. Of course, some restrictions on encryption can be duly effected by the regulations. The law on the subject is clearly still evolving.

The I.T. (Amendment) Act, 2008 amended the Section 69 and introduce new Section 69A and 69B.

[Section 69] Powers to issue directions for interception or monitoring or decryption of any information through any computer resource (Substituted Vide ITAA 2008):

(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to –

(a) provide access to or secure access to the computer resource, generating, transmitting, receiving or storing such information; or

(b) intercept or monitor or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.
(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

[Section 69 A] Power to issue directions for blocking for public access of any information through any computer resource:

(1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under 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 69B] Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security:

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-
section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(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 subsection (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section,

(i) "Computer Contaminant" shall have the meaning assigned to it in section 43

(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

5.2.6 Protected system

Section 70 of the I.T Act, 2000 provides for, the government to authorize, people to access a specified computer, computer system or computer network which is designated as a, "protected system". By virtue of sub-section (2) only on authorized person has access rights to a protected system.

The purpose of declaring a system as a protected one is that such a system is indeed very valuable for the interest of the nation, national security,
and sovereignty or for public order. If anybody creates havoc with these protected systems it can have telling impact upon the entire nation and day-to-day administration.

Section 70 (3) provides that any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term, which may extend to ten years and shall also be liable to fine. It is very much evident that the severity of punishment is much more here as compared to another two somewhat similar provisions, like section 43 (a) [accesses or secures access to such computer, computer system or computer network] or section 66 [hacking with computer system] of the Act.

Importantly, the aforesaid section will also take into cognizance of unauthorized access by the employee (s) of an undertaking whose computer, computer system or computer network has been notified as a protected system.

It is 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 I.T. Act, 2000. Thus an intentional or an accidental access or attempt to secure access to a protected system get punished under the same term.

What is of importance is how does one define the words "attempts to secure access to a protected systems". The quantum of proof that would be required to prove attempt is uncertain. Also what would constitute "attempt to secure access" is not definite and would depend upon the facts and circumstances of each case.

The I.T. (Amendment) Act, 2008 amended Section 70 and Inserted New Section 70A, 70B.
[Section 70] Protected system (Amended Vide ITAA-2008)

(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.

(Substituted vide ITAA-2008)

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1)

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system. (Inserted vide ITAA 2008)

[Section 70A] National nodal agency. (Inserted vide ITAA 2008)

(1) The Central Government may, by notification published in the official Gazette, designate any organization 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.
Section 70BJ 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)

5.2.7 Penalty for misrepresentation

Section 71 creates a new offence to ensure the sanctity of information that is provided to become a part of the digital signature regime envisaged under the I.T. 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 authority under the I.T. Act, 2000 so as to prevent misuse.

If any Certifying Authority is found guilty of making any misrepresentation or suppressing any material facts, then 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 to everyone, who at the time of misrepresentation or suppression of

---

1 Section 71-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.

2 Misrepresentation means and includes, (a) the positive assertion, in a manner not warranted by the information of the person making it, of that which is not true, though he believes it to be true; (b) any breach of duty which, without an intent to deceive, gains an advantage to the person committing it, or any one claiming under him, by misleading another to his prejudice or to the prejudice of any one claiming under him; and (c) causing, however innocently, a party to an agreement, to make a mistake as to the substance of the thing, which is the subject of the agreement, Section 18 of the Indian contract Act, 1872.
material facts, was in-charge of and was responsible to the 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 persual of section 85 of the I.T. Act, 2000.

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, 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 consequence of revocation of his Digital Signature Certificate in terms of section 38 (2)(a). Similarly, if a Certifying Authority is guilty of an offence under section 71, the licence of the Certifying Authority may also be revoked by the controller under section 25 (1) (a) of the I.T. 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 signature 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.

5.2.8 Penalty for breach of confidentiality and Privacy

Section 72 of the IT Act of 2000 offers some protection for breaches of confidentiality and privacy. Non-consensual disclosure of confidential information is punishable by imprisonment for up to two years, or a maximum

1 The word "electronic" substituted by I.T. (Amendment) Act, 2008.
2 Section 72-Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
fine of approximately one lakh rupees. However, the penalty can be imposed only against, functionaries authorized under I.T. Act to secure access to any electronic resource. To attract the penalty, five requisites must be fulfilled, that, (a) any person under the powers conferred under the I.T. Act, rules or regulations made there under; (a) secures access to any electronic record, book, register, correspondence, information, document or other material; (c) without the consent of the person concerned; (d) discloses such electronic record, book, register, correspondence, information, document or other material; (e) to any other person.1

Section 72 enacts a new offence to preserve and protect the privacy and confidentiality of data and information. 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, who 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 here that the entire I.T. Act, 2000 is silent on the contentious issue of privacy, barring this present section. Also the word 'privacy' does not find mention in the body of section 71 but is not mentioned in its heading.

The I.T. Act, 2000 does not define privacy, it only talks of privacy in the heading of section 72.

A perusal of section 72 shows that it has been drafted in a restrictive manner. It only refer to punish those persons who after having secured access to any electronic record, book, registers, 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 cyber space. Spamming, or the practice of sending unsolicited emails to different persons, has not been mentioned at all in the I.T. Act, 2000.

In addition, into 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 purposes of valuable consideration. The stolen information is then invariably sold to different companies who then send unsolicited emails to the email addresses of different persons. All these varied endeavors are a grave violation of individual's privacy.

However, unfortunately, in India awareness about privacy is at a very low level in the meta world what to say in a cyber space. It is important that the Government should legislate about privacy in cyber space. 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.

I.T. (Amendment) Act, 2008 sub-section 72 A has introduced in the requirement of breach of confidentiality and privacy, a guilty state of mind as 'intentionally'.

5.2.9 Penalty for Publishing Digital Signature Certificate false in certain particulars

It has been set out that, the primary function of a Digital Signature Certificate (DSC) is to serve as a method of, authentication or identification, that a party has signed a document. Section 73 with an objective

1 Section 73 - (1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that-
(a) the Certifying Authority listed in the certificate has not issued it; or
(b) the subscriber listed in the certificate has not accepted it; or
(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
to prevent such occurrences prescribes a penalty for publishing false particulars in a DSC. The particulars where misrepresentation attracts this penalty are prescribed under section 73(1). These are the publication\(^1\) of a DSC as to make it available to any other person with the knowledge that, (a) the Certifying Authority listed in the certificate has not issued it; (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.

Any person who contravenes the provisions of 73 (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.

The sub-section (1) states that if publication of a digital signature certificate is for the purpose of verifying a digital signature created prior to such suspension or revocation, then no offence shall be made out.

5.2.10 Publication for fraudulent purpose

In the section 74\(^2\) the onus is on both the Certifying Authority and subscriber not to create, publish or otherwise make available a digital signature certificate for any fraudulent or unlawful purpose.

One crucial point that should not be missed is that any fraudulent or unlawful activity would be taking place on any of the computer resource [Sec.2 (1) (k)]. The fraudulent or unlawful processes may include alteration, deletion or suppression of the input of certain information contained in the digital signature certificate and its use (fraudulent or unlawful) to further any criminal offence.

---

1 Publication is defined as "the action of making publicly known". The Supreme Court held in Bennett Coleman & Co. v. Union of India, (1972)2 SCC 788, that "publication means dissemination and circulation". In the context of digital medium, the term publication includes dissemination, storage and transmission of information or data in electronic form.

2 Section74- Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
The term publication includes dissemination, storage and transmission of information or data in electronic form. Publication for fraudulent purpose in the sec. 74 would mean dissemination, storage and transmission of 'modified' digital signature certificate with the intent to commit fraud. The expression, "fraudulent purpose or unlawful purpose," is wide enough to include contravention of any law for the time being in force.¹

Penalty for publishing Digital Signature Certificate for fraudulent purpose has been made a non-cognizable and bailable offence. The aforesaid offence is punishable 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 creates a distinct kind of crime, which deals with publication of Digital Signature Certificate for fraudulent purposes, while section 73 of the I.T. Act, 2000 has referred to publication of the Digital Signature Certificates, which are false in certain particulars.

5.2.11 Offences by Companies

Section 85² sub-section (1) introduces the concept of "collective responsibility" of a company. Any contravention committed by a company, the

---

1 Central Jute Mills Ltd. v. Dy. Secretary, Ministry of Finance, 40 Com Cases 102 (Cal-DB)(1970).
2 Section 85 - (1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

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

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation- For the purposes of this section-
(i) "company" means anybody corporate and includes a firm or other association of individuals; and
(ii) "director", in relation to a firm, means a partner in the firm.
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 is held responsible for the contravention and thus, is liable to be prosecuted and punished accordingly. Such person, nevertheless, can absolve himself from liability, if he can prove that the contravention took place without his knowledge\(^1\) or he had exercised all due diligence\(^2\) to prevent the commission of such contravention. But where it is proved that contravention had taken place with the consent or connivance or negligence on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer\(^3\) shall be deemed to be guilty of the contravention and shall be liable to be prosecuted and punished.

5.2.12 Confiscation

Sec. 76\(^4\) highlights that all devices whether computer, computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device which helped in the contravention of any provision of this Act, rules, orders or regulations made there under are liable to be confiscated.

The proviso to the section further highlights that in case of an unauthorized use of computer, computer system, floppies, compact disk, tape drives or any other storage, communication, input or output device leading to contravention of any of the provisions under the Act, the adjudicating court not

---

1 Knowledge here means actual or constructive knowledge.
2 due diligence means reasonable steps taken by a person in order to avoid commission of an offence or contravention.
3 other officers may include persons duly authorized by the Board of the Directors, managing agent, constituted attorney etc.
4 Section 76-Any computer, computer system, floppies, compact disk, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules orders or regulations made there under has been or is being contravened, shall be liable to confiscation: Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening the provisions of this Act, rules, orders or regulations made there under as it may think fit.
to confiscate such devices, if the person in whose possession, power or control such devices have been, establish to the satisfaction of the court that he was in no way responsible for any of the contraventions. In such a case, the court may make such other order authorized by this Act, against the person contravening provisions of this Act, rules, orders or regulations made there under.¹

5.2.13 Penalties or Confiscation not to interfere with other punishments

Sec. 77² lays a mandatory condition, which states that penalties or confiscation not to interfere with other punishments to which the person affected thereby is liable under any other law for the time being in force.

That is, apart from facing the penalty or confiscation under the Act, the person may still be found liable under any other law for the time being in force.

The penalties and the confiscation under the IT Act, 2000 are in addition to and not in substitution with the punishments under any other law. Thus, if a cyber crime is covered under the IT Act, 2000 and the IPC, 1860, both, the accused will be prosecuted and punished, if proved guilty, under both the Acts.

The I.T. (Amendment) Act, 2008 amended Section 77 and introduce new Section 77A, 77B.

[Section 77] Compensation, penalties or confiscation not to interfere with other punishment (Substituted Vide ITAA-2008):

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.

---


² Section 77- 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 A] Compounding of Offences:

(1) 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 section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply.

[Section 77 B] Offences with three years imprisonment to be cognizable:

Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

6. **IT ACT, 2000 V. IT (AMENDMENT) ACT, 2008**

On a comparative analysis of the provisions of the IT Act 2000 and the IT Amendment Act 2008, certain observations and comments have been made herein below:-

(1) **Electronic signatures introduced**- With the passage of the IT (Amendment) Act, 2008 India has become technologically neutral due to adoption of electronic signatures as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures. This is a positive change as India has different segments people and all may not be
technologically adept to understand and use the digital signatures. Therefore, allowing forms of authentication that are simpler to use such as retina scanning can be quite useful in effective implementation of the Act. However, the challenge it poses is accessibility to authentication tools and imparting education to people to use the same. It is a challenging task for the Central government to prescribe conditions for considering reliability of electronic signatures or electronic authentication techniques under Section 3A (2), the procedure for ascertaining electronic signature or authentication under Section 3A(3), the manner in which information may be authenticated by electronic signatures in Section 5. It also involves expenditure as such authentication tools will require purchase, installation & training, particularly in all government departments where it is proposed to be used. Equally challenging will be the drafting of duties of subscriber of electronic signature certificate under Section 40 A of the Act which will need to incorporate security measures subscribers can adopt depending on electronic signature being used for signatures. Further, in a move to secure the flow of data and information on the internet, and promote e-commerce & e-governance, the amended Act in Section 84A has empowered the Central Government to prescribe modes or methods for encryption. These parameters should be laid down in consultation with organizations such as Nasscom and/or governmental agencies that can assist in formulation of necessary standards and related rules.

(2) Corporate responsibility introduced in S. 43A:- The corporate responsibility for data protection is incorporated in S 43A in the amended IT Act, 2000 whereby corporate bodies handling sensitive personal information or data in a computer resource are under an obligation to ensure adoption of ‘reasonable security practices’ to maintain its secrecy, failing which they may be liable to pay damages. Also, there is no limit to the amount of compensation that may be awarded by virtue of this section. This section must be read with Section 85 of the IT Act, 2000 whereby all persons responsible to the company for conduct of its business shall be held guilty incase offence was committed by a company unless no knowledge or due diligence to prevent the contravention is proved.
Insertion of this provision is particular significance to BPO companies that handle such sensitive information in the regular course of their business. This provision is important to secure sensitive data and is hence a step in the right direction. However, the challenge is to first elucidate what we qualify as “reasonable security practices”. The Act in explanation to Section 43A indicates these procedures designed to protect such information from ‘unauthorized access, damage, use, modification, disclosure, or impairment, as may be specified in an agreement between parties’ or as may be specified by any law for the time being in force and in absence of both, as may be prescribed by Central Government in consultation with professional bodies/associations. The law explaining the definition of ‘reasonable security practices’ is yet to be laid down and/or Central government is yet to frame its rules thereon. Perhaps, we can take guidance from certain foreign laws on data protection & standards laid down in European Union or by organizations such as OECD in protection of sensitive personal data. It is a challenge for the Central Government to prescribe in consultation with professional bodies the information that will fall within the meaning of “sensitive personal data or information”. To describe what these parameters should be is beyond the scope of this Article but is an interesting issue for discussion.

(3) Critique on amended section 43 of IT Act:- The amended Act provides the distinction between ‘contravention’ and ‘offence’ by introduction of the element of mens rea for an offence (s 43 for contraventions and s 66 of the Act for offences). It is pertinent to note that no ceiling limit for compensation is prescribed under s 43 of the Amendment Act, 2008 which was one crore rupees in the IT Act. The removal of the ceiling limit can be misused or abused particularly seen in instances where company files frivolous claims against its ex-employee who may have joined a competitor firm without breaching its employment contract.

In my opinion, one major diversion from the earlier IT Act is the fact that the amended Section 43 has the insertion of Section 43 (i) & (j) in the amended Act which may require an element of mens rea with actus reus. Particularly Section 43(j) requires presence of mens rea (please note use of words ‘stealing’ and ‘intention to cause damage’ in the section) and the same acts mentioned in section
43 when committed ‘dishonestly’ or ‘fraudulently’ are punishable under amended Section 66. The intent behind this change is to not only punish the offender for its criminal act but also to compensate the victim with pecuniary damages for loss incurred due to acts of the offender. In my view this is a positive change since a ceiling on compensation that may be awarded in s. 43 renders at risk those companies that invest huge amounts of money in their research & development and an employee simply steals way that valuable information or resource by electronic means without due remedy or award of compensable damages.

The relevant provision is as under-

“If any person without the permission of the owner or any other person who is in-charge of a computer, computer system or network…. Steal, causes, 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.”

The intention of the amended Act is to introduce the element of intention in this clause of the Section and this mens rea element also finds its roots in Section 66 where a person will be sentenced if he does the same act ‘dishonestly’ or ‘fraudulently’ within the meaning of IPC i.e. with intention to defraud or cause wrongful loss. ‘Intention to cause damage’ in S.43(j) can be said to also include intention to cause wrongful loss. Per se ‘stealing’ cannot be done without the mens rea in place and therefore this act should fall under s.66 and not 43 incase S.43 is to cover only acts done inadvertently or by negligence. This certainly cannot be the intention/objective of the amendment. Hence, a clarification on this point is necessary.

(4) **Important definitions added**: Two very important definitions are added to the IT Act through IT Amendment Act, 2008- Section 2(ha)- “Communication device” and Section 2 (w)”intermediary”. Although cell phones and other devices used to communicate would fall under the definition of computer in the IT Act. This amendment removes any ambiguity and brings within the ambit of the
Act all communication devices, cell phones, iPods or other devices used to communicate, send or transmit any text, video, audio or image. The insertion of definition of ‘intermediary’ similarly clarifies the categories of service providers that come within its definition that includes telecom service providers, network service providers, internet service provider, webhosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes.

(5) **Legal validity of electronic documents re-emphasized:** Two new sections Section 7A and 10A in the amended Act reinforce the equivalence of paper based documents to electronic documents. Section 7A in the amended Act makes audit of electronic documents also necessary wherever paper based documents are required to be audited by law. Section 10A confers legal validity & enforceability on contracts formed through electronic means. These provisions are inserted to clarify and strengthen the legal principle in Section 4 of the IT Act, 2000 that electronic documents are at par with electronic documents and e-contracts are legally recognized and acceptable in law. This will facilitate growth of e-commerce activity on the internet and build netizen’s confidence.

(6) **Critique on Power of Controller under the amended Act:** Section 28 of the Act provides that the Controller or any authorized officer shall investigate ‘any contravention of the provisions of this Act, rules or regulations made there under’.

These words should be replaced with words ‘any contravention of the provisions of this Chapter’ in light of the fact that the amendment in Section 29 for Controllers power to access computers and data has been curtailed by removal of words “any contravention of the provisions of this Act, rules or regulations made there under” for insertion of words" any contravention of the provisions of this Chapter”. Also, the Controller’s power cannot mean to overlap with Adjudicating officers who are authorized to adjudicate on cases of contravention that fall under Section 43 or the subject matter jurisdiction of CAT or the Police. Therefore, the power of Controller has to be interpreted keeping in view the intent & objectives of the Act which can be clarified.
The role of the Controller to act as repository of digital signatures has been repealed by the IT Amendment Act, 2008. This role has now been assigned to the Certifying Authority in Section 30 of the IT Act. This change poses a major challenge to ensuring the secrecy and privacy of electronic signatures is maintained. The Certifying authorities will bear greater responsibility and need to strengthen their security infrastructure to ensure its role as repository is delivered with efficacy. It will need to allocate more resources and manpower to regularly publish information regarding its practices, electronic signatures certificates and publish the current status of each certificate.

(7) The Role of Adjudicating officers under the amended Act:- The Adjudicating officer’s power under the amended Act in Section 46 (1A) is limited to decide claims where claim for injury or damage does not exceed 5 crores. Beyond 5 crore the jurisdiction shall now vest with competent court. This has introduced another forum for adjudication of cyber contraventions. The words ‘competent court’ also needs to be clearly defined. As per Section 46(2), the quantum of compensation that may be awarded is left to the discretion of Adjudicating officers. This leaves a wide room for subjectivity and quantum should be decided as far as possible objectively keeping in view the parameters of amount of unfair advantage gained amount of loss caused to a person (wherever quantifiable), and repetitive nature of default. The Information Technology (qualification and experience of adjudicating officers and manner of holding enquiry) Rules, 2003 lay down the scope and manner of holding inquiry including reliance on documentary and other evidence gathered in investigations. The rules also provide for compounding of contraventions and describe factors that determine quantum of compensation or penalty.

In the IT Act, 2000 the office of adjudicating officer had the powers of civil court and all proceedings before it are deemed to be judicial proceedings. A new change is incorporated in Section 46(5)(c) whereby the Adjudicating officers have been conferred with powers of execution of orders passed by it, including order of attachment and sale of property, arrest and detention of accused and appointment
of receiver. This empowers the office of Adjudicating Officer and extends greater enforceability and effectiveness of its orders.

(8) Composition of CAT:- The amended Act has changed the composition of the Cyber Appellate Tribunal. The Presiding officer alone would earlier constitute the Cyber Regulations Appellate Tribunal which provision has now been amended. The tribunal would now consist of Chairperson and such number of members as Central Government may appoint. The qualifications for their appointment, term of office salary, power of superintendence, resignation and removal, filling of vacancies have been incorporated. The decision making process allows more objectivity with Section 52 D that provides that the decision shall be taken by majority.

It is pertinent to note that there has not been any amendment in Section 55 by 2008 amendments which states that no order of CAT shall be challenged on ground that there existed a defect in constitution of appellate tribunal. However, in my view this runs contrary to principles of natural justice. An analogy is drawn to Arbitrations where defect in constitution of a tribunal renders an award subject to challenge as per Indian laws.

(9) New cybercrimes as offences under amended Act:- Many cybercrimes for which no express provisions existed in the IT Act, 2000 now stand included by the IT (Amendment) Act, 2008. Sending of offensive or false messages (s 66A), receiving stolen computer resource (s 66B), identity theft (s 66C), cheating by personating (s 66D), violation of privacy (s 66E). A new offence of Cyber terrorism is added in Section 66 F which prescribes punishment that may extend to imprisonment for life. Section 66 F covers any act committed with intent to threaten unity, integrity, security or sovereignty of India or cause terror by causing DoS attacks, introduction of computer contaminant, unauthorized access to a computer resource, stealing of sensitive information, any information likely to cause injury to interests of sovereignty or integrity of India, the security, friendly relations with other states, public order, decency, morality, or in relation to contempt of court, defamation or incitement to an offence, or to advantage of any foreign nation, group of individuals or otherwise. For other offences mentioned in
Section 66, punishment prescribed is generally upto three years and fine of one/two lakhs has been prescribed and these offences are cognizable and bailable. This will not prove to play a deterrent factor for cyber criminals. Further, as per new S. 84B, abetment to commit an offence is made punishable with the punishment provided for the offence under the Act and the new S. 84C makes attempt to commit an offence also a punishable offence with imprisonment for a term which may extend to one-half of the longest term of imprisonment provided for that offence.

In certain offences, such as hacking (s 66) punishment is enhanced from 3 years of imprisonment and fine of 2 lakhs to fine of 5 lakhs. In S. 67, for publishing of obscene information imprisonment term has been reduced from five years to three years (and five years for subsequent offence instead of earlier ten years) and fine has been increased from one lakh to five lakhs (rupees ten lakhs on subsequent conviction). Section 67A adds an offence of publishing material containing sexually explicit conduct punishable with imprisonment for a term that may extend to 5 years with fine upto ten lakhs. This provision was essential to curb MMS attacks and video vouyerism. Section 67B punishes offence of child pornography, child’s sexually explicit act or conduct with imprisonment on first conviction for a term upto 5 years and fine upto 10 lakhs. This is a positive change as it makes even browsing and collecting of child pornography a punishable offence.

Punishment for disclosure of information in breach of lawful contract under sec 72 is increased from 2 yrs upto 5 yrs and from one lakh to 5 lakh or both. This will deter the commission of such crime. By virtue of Section 84 B person who abets a cybercrime will be punished with punishment provided for that offence under the Act. This provision will play a deterrent role and prevent commission of conspiracy linked cybercrimes. Also, punishment for attempt to commit offences is given under Section 84 c which will be punishable with one half of the term of imprisonment prescribed for that offence or such fine as provided or both.

10) **Section 67 C to play a significant role in cyber crime prosecution:**

Section 67 C brings a very significant change in the IT Act, 2000. According to
this section, intermediaries shall be bound to preserve and retain such information as may be prescribed by the Central government and for such duration and format as it may prescribe. Any intermediary that contravenes this provision intentionally or knowingly shall be liable on conviction for imprisonment for a term not exceeding 2 yrs or fine not exceeding one lac or both.

Many cybercrime cases cannot be solved due to lack of evidence and in many cases this is due to the fact that ISP failed to preserve the record pertaining to relevant time. This provision is very helpful in collection of evidence that can prove indispensable in cybercrime cases.

11) **Section 69- Power of the controller to intercept amended:**- Section 69 that deals with power of Controller to intercept information being transmitted through a computer resource when necessary in national interest is amended by Section 69. In fact the power vests now with the Central Government or State Government that empowers it to appoint for reasons in writing, any agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource. This power is to be exercised under great caution and only when it is satisfied that it is necessary or expedient to do so in interests of 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. The procedure and safeguards to exercise this power are laid out by the Information Technology (procedure and safeguards for interception, monitoring and decryption of Information) Rules, 2009. The subscriber or intermediary that fails to extend cooperation in this respect is punishable offence with a term which may extend to 7 yrs and imposition of fine. The element of fine did not exist in the erstwhile Section 69. The said rules provide ample safeguards to ensure the power in this section is diligently exercised, with due authorization procedures complied with and not abused by any agency/intermediary including maintaining confidentiality and rules for maintaining or destruction of such records.
12) **Power to block unlawful websites should be exercised with caution**: Section 69A has been inserted in the IT Act by the amendments in 2008 and gives power to Central government or any authorized officer to direct any agency or intermediary (for reasons recorded in writing) to block websites in special circumstances as applicable in Section 69. Under this Section the grounds on which such blocking is possible are quite wide. In this respect, the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 were passed vide GSR 781(E) dated 27 Oct 2009 whereby websites promoting hate content, slander, defamation, promoting gambling, racism, violence and terrorism, pornography, violent sex can reasonably be blocked. The rules also allow the blocking of websites by a court order. It further provides for review committee to review the decision to block websites. The intermediary that fails to extend cooperation in this respect is punishable offence with a term which may extend to 7 yrs and imposition of fine. We need to use this power with caution as it has a thin line that distinguishes reasonable exercise of power of Censorship.

13) **Section 69B added to confer Power to collect, monitor traffic data**: As a result of the amendments in 2008, Section 69 B confers on the Central government power to appoint any agency to monitor and collect traffic data or information generated, transmitted, received, or stored in any computer resource in order to enhance its cyber security and for identification, analysis, and prevention of intrusion or spread of computer contaminant in the country. The Information Technology (procedure and safeguard for monitoring and collecting traffic data or information) Rules, 2009 have been laid down to monitor and collect the traffic data or information for cyber security purposes under Section 69B. It places responsibility to maintain confidentiality on intermediaries, provides for prohibition of monitoring or collection of data without authorization. This prescribes stringent permissions required to exercise the powers under this Section which are fully justified as abuse of this power can infringe the right to privacy of netizens. It also provides for review of its decisions and destruction of records.
The intermediary that fails to extend cooperation in this respect is punishable offence with a term which may extend to 3 yrs and imposition of fine.

14) **Significance of the term “Critical Information Infrastructure”:**
Section 70 has a very important definition added by the IT (amendment) Act, 2008. The explanation to Section 70 defines what is “critical information infrastructure”. It encompasses the computer resource the destruction of which not only has an adverse impact on defence of India but also economy, public health or safety. This is very significant step as today our IT infrastructure may also be used to manage certain services offered to public at large, destruction of which may directly affect public health and safety. Hence, their protection is equally important as is the maintaining of security and sovereignty of India.

By virtue of Section 70 A and B Indian CERT has been appointed as the National nodal agency for critical information infrastructure protection. The CERT shall play an indispensable role in maintaining cyber security within the country. A very important step is coordination between CERT and service providers, data centre's, body corporate, and other persons (Section 70B(6)). That will lead to effective performance of the role of CERT in. It has multiple roles education, alert system, emergency response, issuing guidelines, reporting of cyber incident amongst other functions. In case any person fails to comply with its directions, such person shall be punishable with imprisonment of term that may extend to one year and fine of one lakh or both. It also excludes the court from taking cognizance of any offence under this section except on a complaint made by authorized officer of CERT to prevent misuse of the Section.

15) **Important clarifications on the Act’s application & effect:**
By virtue of Section 77 in the amended Act, it has been clarified that awarding of compensation, penalty imposed or confiscation made under this Act shall not prevent the award of compensation, or imposition of any other penalty or punishment under any law for the time being in force. This Section can be read with Section 81 proviso wherein it is clarified that IT Act shall not restrict any person from exercising any right conferred under copyright Act, 1957 or patents Act, 1970.
16) The combined effect of Section 77 and 77B:- By virtue of Section 77 Compounding of offences other than offences for which imprisonment for life or punishment for a term exceeding has been provided has been made possible. Section 77 B makes offences punishable with imprisonment of three years and above as cognizable and offence punishable with 3 years of punishment as bailable. Since the majority of cyber crime offences defined under the amended IT Act are punishable with imprisonment for three years, the net effect of all amendments is that a majority of these cybercrimes are bailable. This means that the moment a cybercriminal is arrested by the police, barring a few offences, in almost all other cyber crimes, he has to be released on bail as a matter of right, by the police. A cyber criminal, once released on bail, will immediately attempt at destroying or deleting all electronic traces and trails of his having committed any cyber crime. This makes the task of law enforcement agencies extremely challenging.

17) Combined effect of Section 78 & 80:- The Section 78 of the Act is amended to confer power to investigate offences under the Act from DSP level to Inspector level. This will be instrumental in quicker investigation in the cybercrime cases provided adequate tools and training is provided.

Section 80 has been amended and power to enter and search in a public place is now vested in any police officer not below the rank of inspector or any authorized officer of central government or state government. Such officer is empowered to arrest without warrant a person found therein who is reasonably suspected of having committed or of committing or being about to commit any offence under this Act. However, this section may be misused easily. Unless it is reasonably suspected that a person has committed, is committing or is about to commit an offence, he should not be arrested without warrant. Otherwise cybercafes, in particular could be adversely affected.

18) Liability of Intermediary amended:- The earlier section 79 made network service providers liable for third party content only when it fails to prove that the offence was committed without his knowledge or that he had exercised due diligence to prevent the commission of such offence or contravention. The
burden of proof was on the network service provider. The amended Section 79 states that the intermediary shall not be liable for any third party information if it is only providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted or the intermediary does not initiate the transmission, select the receiver and select or modify the information contained in transmission. It provides that the Intermediary shall be liable if he has conspired or abetted or induced, whether by threats or promise or otherwise in the commission of the unlawful act (Section 79(3)(a)). However, it is pertinent to note that the onus to prove conspiracy has now shifted on the complainant. This may be extremely difficult for a complainant to prove.

Section 3 (b) renders an intermediary liable in case upon receiving actual knowledge or on receiving notice from a government agency, the intermediary fails to expeditiously remove or disable access to the unlawful material without vitiating the evidence in any manner.

19) Examiner of Electronic Evidence created:- With amendments in 2008, Section 79 A is added that empowers the Central government to appoint any department or agency of Central or State government as Examiner of Electronic Evidence. This agency will play a crucial role in providing expert opinion on electronic form of evidence. The explanation to the Section has an inclusive definition of “electronic form evidence” that means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines. With the increasing number of cybercrime cases it will become necessary to set up at least one Examiner of Electronic Evidence in each State. The CFSIL laboratory in Hyderabad is playing similar role at present in cybercrime cases where forensic study of hard discs and other computer accessories, digital equipment is undertaken to provide expert opinion on the digital evidence analyzed.

20) Combined effect of Section 79 and 81- Section 79 has been modified to the effect that an intermediary shall not be liable for any third party information
data or communication link made available or hosted by him. This is however subject to following conditions:

- 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;
- the intermediary does not initiate the transmission or select the receiver of the transmission and select or modify the information contained in the transmission;
- the intermediary observes due diligence while discharging his duties.

As a result of this provision, social networking sites like Facebook, Twitter, Orkut etc. would be immune from liability as long as they satisfy the conditions provided under the section. Similarly, Internet Service Providers (ISP), blogging sites, etc. would also be exempt from liability.

However, an intermediary would lose the immunity, if the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act. Sections 79 also introduced the concept of "notice and take down" provision as prevalent in many foreign jurisdictions. It provides that an intermediary would lose its immunity if upon receiving actual knowledge or on being notified that any information, data or communication link residing in or connected to a computer resource controlled by it is being used to commit an unlawful act and it fails to expeditiously remove or disable access to that material.

Even though the intermediaries are given immunity under Section 79, they could still be held liable under Section 72A for disclosure of personal information of any person where such disclosure is without consent and is with intent to cause wrongful loss or wrongful gain or in breach of a lawful contract. The punishment for such disclosure is imprisonment extending upto three years or fine extending to five lakh rupees or both. This provision introduced under IT Amendment Act, 2008, is aimed at protection of privacy and personal information of a person.
The most controversial portion of the IT Amendment Act 2008 is the proviso that has been added to Section 81 which states that the provisions of the Act shall have overriding effect. The proviso states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 and the Patents Act, 1970. This provision has created a lot of confusion as to the extent of liability provided under section 79.

Section 79 under IT Amendment Act, is purported to be a safe harbor provision modeled on the EU Directive 2000/31. However, Information Technology Amendment Act 2008 left a lot to be desired. Both EU and USA provide specific exclusion to internet service providers under the respective legislations. In order to clarify the issue and put the controversy to rest, Indian legislators need to insert a similar provision proving immunity to ISP in the Copyright Act, 1957.

It is interesting to note that even auction sites, search engines and cyber cafes fall within definition of intermediaries. There is no parallel legislation in the world which provides immunity to such a wide range of intermediaries. This can be reason behind addition of proviso to Section 81. Nevertheless, Information Technology Amendment Act 2008 makes a genuine effort to "provide immunity to the intermediaries but has failed to achieve its objective due to lose drafting of few provisions. Indian Legislators need to plug in these gaps and provide indispensable immunity to the ISPs to enable them to operate in India without any fear and inhibitions".

7. ELECTRONIC EVIDENCE

In any suit or proceeding in a court of law, the judge will be able to resolve it by considering the matter placed before him or her. In the adversarial system of judicial enquiry both the competing counsels adduce evidence trying to convince the judge about their respective viewpoints as to a disputed fact. Evidence could include oral testimony, documents, instruments or weapons used for committing a crime or those that are indicative or related to the offence. Evidence is an integral part of day-to-day life and it inherently possesses a demonstrative character. The
process of objective verifiability lends authenticity to an assertion of fact. It also helps people to reason out facts and arrive at a rational decision.

Since the outcome of a judicial proceeding depends upon the evidences produced before the forum and admitted by the forum, it is necessary to ensure that the process of adducing evidence has followed certain established principles. These principles constitute the law of evidence. Law, as an instrument of regulation, outlines the framework within which the evidences are to be adduced before concerned forum so as to facilitate the judge in forming a rational conclusion on existence or non-existence of a disputed fact. The law of evidence is to be applied where there is a contest as to existence and non-existence of a fact.

In the computer based evidences, generally there are two types of evidences which are produced before the court-

a. Physical evidence
b. Technological evidences

In physical evidences, the investigating officer generally uplifts it from the scene of crime or in the organization itself where the occurrence happened to be. But since the technological evidence is highly sensitive evidence, it must be kept in a climate controlled environment and dust free area.

7.1 Meaning of Evidence

Evidence simply means anything, which is necessary to prove a particular fact. The meaning of the word "evidence" in its legal context is given in the Oxford English Dictionary as-

"Information, whether in the form of personal testimony, the language of documents or the production of material objects, that is given in legal investigation to establish the fact or point in question".

According to section 3 of the Indian Evidence Act, 1872, "Evidence" means and includes-
All statements which court points or requires to be made before it by witnesses, in relation to matters of fact under inquiry, such statements are called oral evidence;

All documents including electronic records produced for the inspection of the court; such documents are called documentary evidence.

It can be observed that Evidence is the means by which the court is put in possession of the facts upon which it has to adjudicate.

7.2 Admissibility\(^1\) of Computer/Electronic Evidence

The information Technology Act, 2000 have carried out necessary amendments in the Indian Evidence Act, 1872. Most important among the amendments is the insertion of Section 65A and 65 B containing special provisions as to evidence relating to electronic records. These Sections are as follows:

**Section 65 A: Special Provisions as to Evidence Relating to Electronic Record:**

The contents of electronic records may be proved in accordance with the provisions of Section 65B.

**Section 65B: Admissibility of Electronic Records:**

(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the

---

\(^1\) Section 136 of the Indian Evidence Act empowers a judge to decide as to the admissibility of evidence produced before him. When either party proposes to give evidence of any fact, the judge may ask the party in what manner the alleged fact, if proved, would be relevant, and the judge can admit evidence only if he thinks that the fact, if proved, would be relevant, and not otherwise. If the admissibility of the proposed fact depends upon proof of some other fact, such last mentioned fact must be proved before evidence is given of the fact first mentioned, unless the party undertakes to give proof of such fact and the judge is satisfied with such undertaking. However, if the relevancy of one fact depends upon another fact being proved first, the judge has the discretion to either permit evidence of the first fact to be given before the second fact is proved or to require that evidence be given of the second fact before evidence is given of the first fact.
information and computer in question and shall be admissible in any
proceedings, without further proof or production of the original, as
evidence of any contents of the original or of any fact stated therein or
which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer
output shall be the following, namely:-

(a) The computer output containing the information was produced by
the computer during the period over which the computer was used
regularly to store or process information for the purposes of any
activities regularly carried on over that period by the person having
lawful control over the use of the computer;

(b) During the said period, information of the kind contained in the
electronic record or of the kind from which the information so
contained is derived was regularly fed into the computer in the
ordinary course of the said activities;

(c) Throughout the material part of the said period, the computer was
operating properly or, if not, then in respect of any period in which
it was not operating properly or was out of operation during the part
of the period, was not such as to affect the electronic record or the
accuracy of its contents; and

(d) The information contained in the electronic record reproduces or is
derived from such information fed into the computer in the ordinary
course of the said activities.

(3) Where over any period, the functions of storing or processing information
for the purposes of any activities of any regularly carried on over that
period as mentioned in clause (a) of sub-section (2) was regularly
performed by computer, whether-

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or
(c) by different combinations of computers operating in succession over that period; or
(d) in any other manner involving the successive operation over the period, in whatever order, of one or more computers and one or more combinations of computers.

all the computer used for that purpose during the period shall be treated for the purposes of this section as constituting a single computers; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say-

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;
(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purpose of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,-

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated
otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

**Explanation**- For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process;

In India, case laws are yet to develop in this field. In USA, courts have dealt this aspect in detail and followed two different lines in admitting the computer-generated evidence. Firstly, the courts generally have admitted computer records upon a showing that the records fall within the business records exception under Federal Rule of Evidence 803(6), which states as follows:

**Records of regularly conducted activity**- A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

Applying this test, the courts have indicated that computer records generally can be admitted as business records if they were kept pursuant to a routine procedure for motives that tend to assure their accuracy.\(^1\)

\(^1\) *United States v. Salgado*, 250 F.3d 438, 452 (6th Cir.2001); *United States v. Cestnik*, 36 F.3d 904, 909-10 (10th Cir.1994); *United States v. Moore*, 923 F.2d 910, 914 (1st Cir. 1991); *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990).
The second rule of admissibility of computer records in US is based on the assumption that they are hearsay evidence. When a computer record contains the assertions of a person, whether or not processed by a computer, and is offered to prove the truth of the matter asserted, the record can contain hearsay. However this is not a very happy situation since the very definition of hearsay evidence is not applicable to a computer-recorded document, unlike a document entered by a human being. There are many system generated documents such log files and these are not mere hearsay but concrete evidence of a happening.\(^1\) The evidentiary issue is no longer whether a human's out-of-court statement was truthful and accurate (a question of hearsay), but instead whether the computer program that generated the record was functioning properly (a question of authenticity).\(^2\) For example, a suspect in a fraud case might use a spreadsheet program to process financial figures relating to the fraudulent scheme. A computer record containing the output of the program would derive from both human statements (the suspect's input to the spreadsheet program) and computer processing (the mathematical operations of the spreadsheet program). Accordingly, the record combines the evidentiary concerns raised by computer-stored and computer-generated records. The party seeking the admission of the record should address both the hearsay issues implicated by the original input and the authenticity issues raised by the computer processing.

7.3 Effect of Electronic Evidence

The question that arises is the weight age that should be given to such e-evidence. Once admitted, an evidence could be challenged on various grounds, inter alia, lack of integrity, lack of relevance to the issue or that which has been tampered with etc. To prove such deficiency is the burden of the opponent of the evidence, while the proponent may lead evidence in support of the accuracy and weight of the record. This is particularly important in respect of digital data which can be tampered without leaving a clue of such tampering. In such cases, the only resort is to establish complete link up chain of custody of the data to ensure the

integrity of the data is being produced in evidence, usually; systems manager of the proponent is called upon to testify the accuracy of the document. The Indian IT Act 2000 legislates on a connected aspect through an amendment brought about in the Indian Evidence Act through s 85B which is as follows:

**Section 85B Presumption as to electronic records and electronic signatures—**

(1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure electronic signature, the Court shall presume unless the contrary is proved that-

(a) the secure electronic signature is affixed by subscriber with the intention of signing or approving the electronic record;

(b) except in the case of a secure electronic record or a secure electronic signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any electronic signature.

Hence, there is a presumption as to authenticity of electronic records in case of secure electronic records. Other electronic records can be proved by adducing evidence and presumption will not operate in case of documents which do not fall under the definition of secure electronic records. It is pertinent to point out herein that with the passage of the Information Technology (Amendment) Act 2008, India would become technologically neutral due to adoption of electronic signatures as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures.

---

The UNCITRAL Model Law in art 9(2) states as follows:

Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

One drawback of setting up discretionary guidelines in a statute is that those delineated factors become minimum requirement. Opponents of this view on the other hand, believe that the statute should not give guidance on the factor which will weigh the substance of evidence.

7.4 Appreciation of Computer Generated Evidence by Judiciary

The tools and techniques can help the investigating agencies in gathering the electronic evidence in cyber crimes. However, their success in prosecuting the criminals equally depend on the capability of the judiciary in appreciating the computer generated evidence. A judiciary that is accustomed to receiving tangible evidences may have some problems in adapting to receiving logical evidence. Thus there is a need for the judiciary too to build their capacity in understanding and appreciating the computer generated evidence as and when they are produced in the court. It is needless to say that acquiring a minimum level of knowledge in the computer and network terminology and technology is a must for the judiciary in this developing cyber age.

Indian Information Technology Act, 2000\(^1\) provides for a mechanism in which the Central Government is empowered to appoint adjudicating officers who has experience in both information technology and legal or judicial fields, for adjudicating on any contraventions of the provisions, of or made under the Act. It also provide for the constitution of a Cyber Regulations Appellate Tribunal for hearing the appeals from the orders of the adjudicating officers. By these provisions, the Act provides for adjudication of contraventions of cyber

\(^{1}\) Sections 46 and 48.
regulations by people with specialized knowledge. However, this does not exonerate judiciary from preparing itself to deal with cyber evidence, because such evidence is not limited to contraventions of cyber regulations but extend to entire criminal as well as civil law administration.

When we talk about the appreciation of computer generated evidence by the judiciary it goes without saying that all those professionals associated with administration of justice needs to become familiar with the technicalities. The role of prosecutors and the defense lawyers in evaluating and presenting such evidence in a court of law cannot be over emphasized. Unless they are thorough they will not be in a position to make the judge to appreciate the evidentiary value of the document of data produced.

8. JURISDICTION IN CYBER SPACE

While the world we live in is physically demarcated in boundaries and territories, the world of cyber space does not recognize and physical or political barriers or national frontiers. In plain words, cyber world is transnational, a global medium devoid of any territorial divisions. Internet has made its place in today's world as an important and powerful medium of communication, information exchange e-commerce.

The unbounded nature of the Internet has challenged the basis for the traditional nations of jurisdiction which are predicated upon real space demarcation. Because a page on a worldwide web can reach web surfers in every state in the nation and perhaps every nation on the earth, there arises the issue of where exactly a person who has a cause of action, based upon a web transaction may sue. The place of the residence of the defendant or the cause of action of the suit, which are the traditional basis for fixing jurisdiction, cannot be established with certainty in the Internet.

8.1. Definition of Jurisdiction

In simple words, jurisdiction is the power of a court to hear and determine a case. Without jurisdiction, a court's judgment is ineffective and imponent.

According to Black’s Law dictionary ‘jurisdiction’ is defined as the power of the court to decide a matter in controversy and presupposes the existence of a duly constituted court with control over the matter and the parties. However with the passage of time and developments in the economic world, courts were rather compelled to find out adequate and effective alternatives to the above-mentioned meaning.

Jurisdiction is essentially of two types, namely subject matter jurisdiction and personal jurisdiction, and these two must be conjunctively satisfied for a judgment to take effect.

8.2 Cyber Jurisdiction

The Internet can be seen as multi-jurisdictional because of the ease which a user can access a web site anywhere in the world. It can even be viewed as a jurisdictional in the sense that from the user's perspective state and national borders are essentially transparent. For courts determining jurisdiction, however, this situation is more problematic.

The developing law of jurisdiction must address whether a particular event in cyberspace is controlled by the laws of the state or country where the Website is located, by the laws of the state or country where the Internet service provider is located, by the laws of the state or country where the user is located, or perhaps by

---

1 Subject matter jurisdiction is defined as the competence of the court to hear and determine a particular category of cases. It requires a determination of whether a claim is actionable in the court where the case is filed.

2 Personal jurisdiction is simply the competence of the court to determine a case against a particular category of persons. It requires a determination of whether the person is subject to the court in which the case is filed.


all of these laws.¹ A number of commentators have voiced the notion that
cyberspace should be treated as a separate jurisdiction.² In practice, this view has
not been supported by the Courts or addressed by law-makers.

Cyber jurisdictional issues have been dealt with primarily in the civil
courts. Since the advent of *U.S. v. Thomas*, infra, and *Minnesota v. Granite Gate
Resorts, Inc*, infra, however, cyber jurisdiction issues have begun to be examined
in criminal courts as well.

**8.2.1 Cyber Jurisdiction in Civil Cases**

In determining whether jurisdiction exists over a defendant, the U.S.
Federal courts apply the law of the forum state, subject to the limits of the Due
Process Clause of the Fourteenth Amendment.

However, other issues dealing with cyber jurisdiction remain unsettled. For
example, the United States District Court of Connecticut held that the continuous
availability of an Internet advertisement containing an 800 number was enough to
establish jurisdiction while the United States District Court of Southern District of
New York held that having an Internet advertisement containing an 800 number
was not enough to establish jurisdiction.

In *Bensusan Restaurant Corp. v. King*, the plaintiff, operator of the New
York jazz club, The Blue Note, complained that the defendant had infringed on its
rights by using its trademark. Defendant, owner and operator of a small club called
The Blue Note, in Columbia, Missouri, had created a Web page which allowed
users to order tickets to attend the club's shows. The court had to decide whether
the creation of a Web site in Missouri containing a telephone number was an offer
to sell to citizens in New York.

The defendant argued the court lacked personal jurisdiction under New
York's long-arm statute. He defended that all he had done was set-up a Web site in

---

1 Stuart Biegel, "Indictment of CompuServe Official in Germany Bring Viletable Issues of
Cyber Jurisdiction into Force", http://www.gse.ucla.edu/iclp/apr97.html
2 David R. Johnson and David Post, "Law and Border – The Rise of Law in Cyberspace",
Missouri aimed at Missouri residents. Furthermore, any tickets sold over the Internet to users had to be picked up either at ticket outlets in Columbia, Missouri, or at the club on the night of the show.

The court agreed finding that it took several affirmative steps to obtain access to the Web site and use the information there. The court also ruled that there was no proof that the defendant had directed any infringing activity at New York. The court held that merely because someone can access information on the Internet about an allegedly infringing product, it is not equivalent to a person selling, advertising, promoting or otherwise attempting to target that product in New York.

Under Due Process, in order for the court to exercise personal jurisdiction, it must be shown that the defendant had purposefully established minimum contact with the forum state such that the maintenance of the suit did not offend the traditional notions of fair play and substantial justice. The court ruled that the defendant's simple creation of a Web site, that was available to any user who can find it on Internet, was not an act of purposeful availment of the benefits of the state of New York. Creating a Web site was similar to placing a product into the stream of commerce. The Web site's effect may be felt nationally or even internationally, but this without more, was not enough to establish an act that was purposefully directed toward the forum state. Based on these rulings the Court held that an exercise of personal jurisdiction would violate the protections of the Due Process Clause.

Inset Systems, Inc. v. Instruction Set, Inc., is a case where Inset Systems, Inc. ("Inset"), a Connecticut corporation, discovered that Instruction Set, Inc. ("ISI") a Massachusetts corporation, had infringed on its trademark by using the

1 Ibid, at 299.
2 Ibid.
domain address INSET.COM and the telephone number 1-800-US-INSET. ISI moved to dismiss for lack of personal jurisdiction and improper venue. In order to determine jurisdiction the Court had to satisfy the solicitation of business provision of Connecticut's long-arm statute and determine whether ISI had sufficient minimum contacts with the forum state to support the exercise of personal jurisdiction.

Inset contended that Connecticut's long-arm statute conferred jurisdiction over ISI because of its Internet advertisement and the availability of its 800 number. The court agreed and relied upon McFaddin v. National Executive Search, Inc.,\(^1\) and Whelen Eng'g Co. v. Tomar Elecs.,\(^2\) to establish that ISI's advertising over the Internet was solicitation of a sufficient repetitive nature to satisfy Connecticut's long-arm statute.

The court ruled that ISI had been advertising continuously over the Internet to the over 10,000 access sites located in Connecticut. The court also ruled that Internet advertising was not like hard-copy advertisements that had a limited reach and which were normally thrown away after use. Internet advertisements were persistent in nature allowing them to be accessed again and again by a large number of potential readers. The court held that because of the continuous availability of the advertisement on the Internet the defendant was subject to Connecticut's long-arm jurisdiction.\(^3\)

In order to meet Due Process requirements the court had to satisfy two tests. First, that a non-resident corporate defendant has minimum contacts with the forum state such that it would reasonably anticipate being held into court.\(^4\) Second, that maintenance of the suit in the forum state would not offend traditional notions of fair play and substantial Justice.\(^5\) ISI claimed that minimum contacts were lacking. ISI said it did not conduct business in Connecticut on a regular basis, it

\(^2\) 672 F. Supp. 659 (D.Conn. 1987)
\(^3\) Inset, 937 F. Supp. 161 at 164.
did not maintain an office in the state, nor did it have a sales force or employees in the State. Accordingly, ISI argued, the court should find that the minimum contacts test was not satisfied.

Disagreeing, the court ruled that ISI purposefully directed its advertising activities toward Connecticut on a continuing basis by posting its toll-free number on the Internet and directing its advertising activities toward both the state of Connecticut and to the entire United States since March 1995.\(^1\) These actions led the Court to rule ISI had purposefully availed itself of the privilege of doing business by establishing minimum contacts within the state. Consequently, the court reasoned ISI could reasonably anticipate the possibility of being held into court.\(^2\) Thus, the court held that Due Process was satisfied, and that assertion of jurisdiction did not offend the notions of fair play and substantial justice. In support of its holding, it ruled that the relative burdens on the defendant were not unreasonable. The travel time between the defendant and the location of the suit was less than two hours and that the defendant had already retained counsel within the forum state.\(^3\)

Not all commentators agree with the holding of *Inset Systems*, because of the consequences of its logic. Their concern is that if the courts followed *Inset Systems*, the implications are that there would be nationwide, even worldwide jurisdiction over anyone and everyone who created a Web page on the Internet.

Declining to follow *Inset Systems*, the U.S. District Court of the Southern District of New York in *The Hearst Corp.* v. *Goldberger*,\(^4\) ruled that nationwide jurisdiction was inconsistent with traditional personal jurisdiction case law, and as a policy matter it was unacceptable.\(^5\)

The Court in *Zippo Mfg.* v. *Zippo Dot Com, Inc.*,\(^6\) dealt with a cyber squatting case, where the plaintiff sued an Internet news service for trademark dilution, infringement and false designation for using the domain names

\(^1\) Ibid, at 164.  
\(^2\) Ibid, at 165.  
\(^3\) Ibid.  
"zippo.com," "zippo.net," and "zippo-news.com." The court found jurisdiction and held that the likelihood of personal jurisdiction being found can be constitutionally based on an entity's presence on the Internet.\(^1\) The court held that the extent of the entity's presence, in the manner of sliding scale, was directly proportionate to the nature and quality of the commercial activity conducted over the internet. The court found that a passive web site that only made information available to interested users was not grounds for exercising jurisdiction. A web site that entered into contracts and knowingly and repeatedly transmitted computer files would be properly subject to personal jurisdiction. In cases dealing with the middle ground, where interactive web sites exchanged information with a user, the exercise of jurisdiction should be determined by examining the commercial nature of the exchange and the level of interactivity.

8.2.2 Cyber jurisdiction in Criminal Cases

The question of cyber jurisdiction in a criminal case came to the forefront of attention in early 1996 in *U.S. v. Thomas*,\(^2\) when the Sixth Circuit upheld the highly publicized conviction of a couple operating a pornographic bulletin board from their home. The defendants began operating the Amateur Action Computer Bulletin Board System ("AABBS") from their home in Milpitas, California in February 1991. The AABBS contained approximately 14,000 Graphic Interchange Format ("GIF") files. These files could be accessed by members who possessed the password. Once the password was entered, the users were able to select, retrieve, or download the GIF files to their own computers.

The government got involved in AABBS' activities when a Web surfer found the site, explored the introductory screens, was offended and subsequently complained. In 1994, a U.S. Magistrate Judge for the Northern District of California issued a search warrant authorizing a search of the defendant's home. As a result of the evidence found their computer system was confiscated.

The defendants were convicted in the U.S. District Court, Western District of Tennessee on federal obscenity charges. They appealed and the appellate court

\(^1\) Ibid, at 1124.
\(^2\) 74 F.3d 701 (6th Cir. 1996).
affirmed. There were two premises for their appeal: (1) The federal obscenity statute\(^1\) did not apply to intangible objects like computer GIF files, and (2) Congress did not intend to regulate the type of transmissions at issue because the federal obscenity statute did not expressly prohibit such conduct.

The defendants asserted that the GIF files were an intangible string of 0's and 1's which only viewable images became after being decoded in the AABBS member's computer. The court disagreed, ruling that the fashion in which the images were transmitted did not affect their ability to be viewed or printed out by members in Tennessee.\(^2\) The defendants also argued that they were prosecuted under the wrong statute and that their conduct, if criminal at all, fell within the prohibitions of the statute which addresses commercial dial-a-porn operations.\(^3\) The court declined to accept this argument. Instead it ruled that the statute must be construed to affect the intent of Congress, which was to prevent the channels of interstate commerce from being used to disseminate any obscene matter.\(^4\)

\textit{Miller v. California},\(^5\) held obscenity was to be judged by what the average person applying contemporary community standards would find to be obscene. Defendants argued the internet environment provides broad-ranging connections among people in cyber space, as such the notion of obscenity tied to geographic locale would put a chill on protected speech.\(^6\) The defendants asserted a more flexible definition was needed because BBS operators could not select who received their material.

The court ruled that the defendants had a pre-existing method of screening potential members. By pre-screening their members they could protect themselves from being subjected to liability in jurisdictions with less tolerant standards. This could be accomplished by refusing to give passwords to users from those districts. The court further ruled the defendants were free to tailor their messages on a selective basis to the communities it chose to serve. Accordingly, it was held by

\(^{1}\) 18 U.S.C. 1465.
\(^{2}\) \textit{U.S. v. Thomas}, 74 F. 3d at 706.
\(^{3}\) 47 U.S.C. Section 223 (b) (1934, amended 1988).
\(^{4}\) \textit{U.S. v. Thomas}, 74 F. 3d at 708.
\(^{5}\) 413 U.S. 15, 93 S. Ct. 2607,37 L.Ed.2d 419 (1973).
\(^{6}\) Ibid. at 710-11.
the court that there was no need to develop a new definition of community.\textsuperscript{1}

The case turned on the fact that even though the GIF files never actually left Northern California and were arguably not obscene under Northern California, Bay Area standards, they were obscene by the standards of Memphis, Tennessee. The Court applied the community standards of the geographic area where the materials were sent as the proper test, in affirming the lower court's holding that defendants were violating federal obscenity laws.

\subsection*{8.2.3 Cyber jurisdiction in International Cases}

When adjudicating cases involving foreign nationals, the courts must balance several factors. On a case by case basis, the courts must consider the procedural and substantive policies of other countries whose interests are affected by the court's assertion of jurisdiction. Keeping these policies in mind, the court must then consider the reasonableness of assertion of jurisdiction examined in the light of the interest of the federal government in its foreign relation policies. When extending jurisdiction into the international field great care and reserve must be exercised.\textsuperscript{2} Because of these sovereignty concerns, there is a higher jurisdictional barrier when litigating against a foreign national.\textsuperscript{3}

There are no international cyber jurisdiction cases, however, \textit{Asahi Metal Industry Company,} referenced infra and \textit{Core-Vent,} discussed infra can both provide the framework for future cyber jurisdiction cases. \textit{Playboy Enterprises,} infra discusses an international civil case involving trademark infringement. In that case the court sidestepped the issue of international cyber jurisdiction relying on a previous 1981 injunction against the defendant to base its finding of jurisdiction. Nevertheless, the case provides useful insights into the application of cyber jurisdiction principals in international cases. The Supreme Court in \textit{Asahi Metal Industry Company v. Superior Court,}\textsuperscript{4} indicated that a plaintiff seeking to hale a foreign citizen into court in the United States must meet a higher jurisdictional threshold than is required when the defendant is a United States citizen. In \textit{Asahi} the court found that even though Asahi had minimum contacts with the forum state, it would be unreasonable and unfair to find jurisdiction for

\begin{itemize}
\item \textsuperscript{1} \textit{U.S. v. Thomas}, 74 F. 3d at 711.
\item \textsuperscript{2} \textit{Asahi Metal Industry Company v. Superior Court}, 480 U.S. 102 (1987).
\item \textsuperscript{3} \textit{Sinatra v. National Enquirer}, 854 F. 2d at 1199.
\item \textsuperscript{4} 480 U.S. 102 [107 S.Ct. 1026] (1987).
\end{itemize}
three reasons: (1) the distance between defendant's headquarters in Japan and the Superior Court of California and the unique burdens of submitting a dispute between two foreign nationals in a foreign legal system; (2) California's and the foreign plaintiff's slight interest in having the case heard in California; (3) the affect on the procedural and substantive interests of other nations by California's assertion of jurisdiction over a foreign nationals. Commentators have proposed that these international factors were dispositive in the court's decision.

In *Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.*, the issue at bar was whether personal jurisdiction applied in enforcing a court injunction entered June 26, 1981. The court found that jurisdiction applied because of the earlier court injunction where jurisdiction had previously been established. The appeals court upheld the 1981 injunction against the defendant, enjoining it from publishing or distributing its "Playmen" magazine in the United States.

The defendant had a pay Web site located in Italy and accessed by United States residents. Because the users had to subscribe to access the files on the Web page the court ruled the defendant could determine which of its subscribers were United States citizens, and was therefore, knowingly allowing them to access the Web site. Once at the Web site users could download the pictorial images and store them on their computers. Based on these facts the court found the site to be a United States distribution in violation of the injunction. The court ruled that the defendant could not be prohibited from operating its Web site merely because the site was accessible from within a country which had banned its product. The court held that the Internet deserved special protection as a place where public discourse could be held without regard to nationality, religion, sex, age, or to monitors of community standards of decency. Nevertheless, the court continued, this special protection did not extend to ignoring court-orders. If this were allowed injunctions would cease to have meaning and intellectual property would cease to be properly protected.

1 Ibid, at 105-6.
2 Core-Vent Corp. v. Nobel Industries, AB, 11 F. 3d 1482, 1490 (9th Cir. 1993).
4 Ibid, at 1037.
5 Ibid, at 1039-40.
6 Ibid.
8.3 Indian Approach

8.3.1 Jurisdiction by Choice

The autonomy of parties is recognized as one of the fundamental principles of private international law. It is open to parties for their convenience to decide to choose one or more competent courts to decide their disputes if more than one court has jurisdiction to try their case. Incase parties under their own agreement expressly agree that their dispute shall be tried by a particular court, then the parties are bound by the forum selection clause. However, it is settled law that by agreement the parties cannot confer Jurisdiction where none exists except in case of out of court dispute resolution procedures such as arbitration.

8.3.2 Jurisdiction Based on Code of Civil Procedure

According to the Code of Civil Procedure, 1908 pecuniary jurisdiction limits the power of court to hear cases upto a pecuniary limit only (S.6). Jurisdiction also depends on where subject matter is situated (S.16), where suit is for compensation for wrong done to the person or to movable property (S.19) or where defendants reside or cause of action arises (S.20). In *Rajasthan High Court Advocates Association v. Union of India* the Supreme Court elucidated the meaning of 'Cause of action' as every fact which would be necessary for the plaintiff to prove, if traversed, in order to support his right to the judgment of the court. Every fact, which is necessary to prove, as distinguished from every piece of evidence, which is necessary to prove each fact, comprises in "Cause of action". In *Casio India Co. Ltd. v. Ashita Tele Systems Pvt. Ltd.*, the Delhi High Court held that once a website can be accessed from Delhi, it is enough to invoke the territorial jurisdiction of the court. The court held that since the plaintiff does not need to prove actual sale or a particular act of deception in a passing off case it was not required that actual deception should take place in Delhi. Recently in

---

another decision of the Delhi High Court, India TV, Independent News Service Pvt. Ltd. v. India Broadcast Live LLC,¹ the court took the view that mere fact that a website is accessible in a particular place may not itself be sufficient for the courts of that place to exercise personal jurisdiction over the owners of the website. However, where the website is not merely passive but is interactive permitting the browsers to not only access the contents thereof but also subscribe to the services provided by owners/operators, the position would be different. The court observed that even where a website is interactive, the level of interactivity would be relevant consideration and limited interactivity may not be sufficient for a court to exercise jurisdiction. This rationale is fully reasonable and justified and reinforces the reasoning adopted by US courts in cases such as Cybersell Inc and CompuServe’s case.²

8.3.3 Jurisdiction based on Cr. P. C.

Section 75 of the IT Act is restricted only to those offences or contraventions provided therein and not to other offences under other laws such as the Indian Penal Code, 1860. Jurisdiction over other cyber crimes, for instance under the Indian Penal Code, 1860, has to be determined by the provisions of the Criminal Procedure Code, 1973. The fundamental principle on jurisdiction is the same under the IT Act³ and the Criminal Procedure Code, 1973, though stated differently.

The basic legal principle of jurisdiction under the Code of Criminal Procedure, 1973 is that every offence shall ordinarily be inquired into and tried by a court within whose local jurisdiction it was committed.⁴ These principles in the Code of Criminal Procedure, 1973 apply for determining jurisdiction in trial by courts as well as in investigation by the police. In a case where an offence is committed in more places than one, or partly in one place and partly in another, or where it is continuing and continues to be committed in more than one local area,

³ Sec. 1 (2) r/w Sec. 75 of IT Act, 2000
⁴ Sec. 177 of Cr.P.C., 1973

373
or where the offence consists of several acts done in different local areas, then it may be inquired into or tried by a court having jurisdiction over either of such areas.¹ In the event where it is uncertain in which of several areas the offence was committed, again it may be inquired into or tried by a court having jurisdiction over either of such areas of uncertainty.²

In a case where an act is an offence by reason of anything which has been done and of a consequence which has ensued, the offence may be inquired into or tried by a court within whose local jurisdiction such act has been done or such consequence has ensued.³ For instance, in a case of defamation, either of the courts, i.e. of the place from where the defamatory letter was e-mailed and the place at which it was published or received, if different, shall have jurisdiction to inquire and try the same. To cite another instance, where in pursuance of misrepresentation by A through e-mail from place X, property was delivered at place Y, A can be tried for the offence of cheating either at place X or Y. In a case where a person in Bombay does an act of hacking of a computer system located in Delhi, he may be tried either in Bombay or Delhi.

In a case where an act is an offence by reason of its relation to any other act which is also an offence or which would be an offence if the doer was capable of committing an offence, the first mentioned offence may be inquired into or tried by a court within whose local jurisdiction either of the acts was done.⁴ For instance, in a case of manufacture of sub-standard fertilizer in place X which is marketed through e-commerce at place Y, prosecution can be launched at either of the said places because the marketing of the sub-standard fertilizer is an offence by reason of sub-standard manufacture.

Certain specified offences have been required by law to be inquired into or tried in certain places.⁵ For instance, an offence of criminal misappropriation or of criminal breach of trust, may be inquired into or tried by a court within whose

¹ Sec. 178 of Cr.P.C., 1973
² Sec. 178(a) of Cr.P.C., 1973
³ Sec. 179 of Cr.P.C., 1973
⁴ Sec. 180 of Cr.P.C., 1973
⁵ Sec. 181 of Cr.P.C., 1973
local jurisdiction the offence was committed or any part of the property which is
the subject of the offence was received or retained or was required to be returned
or accounted for, by the accused person.\textsuperscript{1} For example, if an employee of a
company based at Delhi, by operating through the Internet the bank account of his
employer company in a Bombay bank, transfers funds to his account at Calcutta,
the case of misappropriation can be tried either at Delhi or Bombay where the
offence was partially committed or at Calcutta where the money was received and
retained.

The law also provides that in the case of any offence which includes
cheating, if the deception is practiced by means of letters or telecommunication
messages, it maybe inquired into or tried by any court within whose jurisdiction
such letters or messages were sent or where the same were received.\textsuperscript{2} Moreover,
any offence of cheating and dishonestly inducing delivery of property may be
inquired into or tried by a court having jurisdiction on the place where the property
was delivered by the person deceived or where it was received by the accused
person.\textsuperscript{3}

In a case where two or more courts take cognizance of the same offence
and a question arises as to which of the courts has jurisdiction to inquie into or try
that offence, this question shall be decided by the High Court, under whose
jurisdiction both such courts function.\textsuperscript{4} However, if the courts are not
subordinate to the same High Court, the question of jurisdiction shall be decided
by the High Court within whose appellate criminal jurisdiction the proceedings
were first commenced.\textsuperscript{5} In such circumstances, all other proceedings with respect
to that offence shall be discontinued.

Where two or more courts have jurisdiction over an offence, the choice of
the court for institution of the case lies with the complainant. He will obviously
choose the forum which is most convenient for him and most inconvenient for the
accused.

\textsuperscript{1} Sec. 181 (4) of Cr.P.C., 1973
\textsuperscript{2} Sec. 182 of Cr.P.C., 1973
\textsuperscript{3} Sec. 182 of Cr.P.C., 1973
\textsuperscript{4} Sec. 186 (a) of Cr.P.C., 1973
\textsuperscript{5} Sec. 186 (b) of Cr.P.C., 1973

375
8.3.4 Jurisdiction under I.T. Act

Section 1(2) of the IT Act has made this Act applicable to whole of India and to any offence or contravention there under committed outside India by any person. Section 75 provides that provisions of the IT Act shall also apply to any offence or contravention committed outside India by any person irrespective of his nationality, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. Therefore, keeping in view the nature of cyber crimes, the IT Act has extended the jurisdiction of the Act beyond national borders. But its implementation depends upon quick response from the other country. Therefore, there is a need to evolve mutual co-operation and strategies the international level and new methods of dispute resolution should give way to the conventional methods.¹

Provisions of this nature are unlikely to be free for a number of reasons. Firstly, it is unfair to suggest that the moment an Indian computer system is used, an a defined by Indian laxvs as an "offence" would be subject to the jurisdiction of India.

To Illustrate, let us consider a web site located in a foreign country. The site may host content that would be perfectly legal in its home country, but may be considered offensive or illegal in India. If an Indian chooses to view this site on a computer situated in India, does that mean that the site can be prosecuted in an Indian court? This would appear to violate principles of Justice. As explained earlier, the judicial trend of examining the amount of activity that a site undertakes in a particular jurisdiction is a far more equitable method to determine jurisdiction.

Further, even if Indian Courts are to claim jurisdiction and pass judgments on the basis of the principle expostulated by the IT Act, 2000, it is unlikely that foreign courts will enforce these judgments since they would not accept the principles utilized by the Act as adequate to grant Indian Courts jurisdiction. This would also reader the Act ineffective.²

In a broad sweep, the Act has adopted the principal of universal jurisdiction to cover both cyber contraventions and cyber offences. It is important to note that the universal jurisdiction over specified offences is often a result of universal condemnation of those activities, and requires co-operation to suppress them, as reflected in widely accepted international agreements or conventions.

Though India is not one of the signatories to Cyber Crime Convention, but it has adopted principal of universal jurisdiction to cover both cyber contraventions and cyber offences under the Act.

It has been argued that from the point of view of application, it would be extremely difficult to enforce the jurisdiction of Indian Courts on cyber criminals belonging to different nationalities. Moreover, the Extradition Treaties, which India has signed so far, do not cover 'cyber crime' as an extraditable offence. Had India being a signatory to the Cyber Crime Convention, then by the virtue of Article 24 of the said Convention the criminal offences a mentioned in Article 2-11 shall be deemed to be included as extraditable offences in any

---

1 A State has jurisdiction to define and prescribe punishment for certain offences recognized by the community of nations as a universal concern, such as piracy, salve trade, attacks on or hijacking of aircraft, genocide, war crimes, terrorism, including instances of cyber terrorism.

2 Convention on Cyber Crime has been opened for signature in Budapest, on 23 November, 2001. Its signatories include 26 European members, United States, Canada, Japan and South Africa.

3 The preamble of the Convention states that the objective is to have a common criminal policy aimed at the protection of society against cyber crime, inter alia by adopting appropriate legislation and fostering international co-operation; it calls for the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international co-operation. The Convention aims principally at (1) harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation.

4 Legislations of the European union which forbid not only its own nationals but also persons wanted by another non-EU countries to be extradited for cases which award the capital punishment. For example, Denmark has refused to hand over Kim Peter Davy, alias Niels Christian Nielsen, the principal accused in the 'Purulia armsdrop case.

Articles 2-11 of the Convention describes criminal offences, like illegal access [Art.2], illegal interception [Art.3], data interference [Art. 4], system interference [Art.5], misuse of devices [Art.6], computer-related forgeries [Art.7], computer-related fraud [Art.8], offences related to child pornography [Art.9], offences related to infringement of copyright and related rights [Art.10] and attempt and aiding or abetting the commission of any of the offences established in accordance with Articles 2-10 of the present Convention with intent that such offence be committed [Art. 11].
extradition treaty existing between or among the parties. Further, the parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

To believe that the Convention would be a panacea to the problem of extraterritoriality is erroneous. Cyber crime involving computer, computer system or computer network, geographically spread across many countries may give rise to difficult jurisdictional issues. A lot will depend on the nature of crime, the 'point of origin' as well as 'point of disruption' and the extent of economic loss.

In R. v. Governor of Brixton Prison and another, ex parte Levin,1 where Citibank faced the wrath of a hacker on its cash management system, resulting in illegal transfer of funds from customers account into the accounts of the hacker, later identified as Vladimer Levin, and his accomplices. Levin was arrested in the United Kingdom and subsequently extradited to the United States.

One of the most crucial jurisdictional issues was the 'place of origin' of the cyber crime. The defence argument was that the criminal act occurred in St. Petersburg at the moment when Levin pressed particular keys on the keyboard resulting into fraudulent Citibank transfers, hence Levin to be tried as per the Russian law. The complainant argued that the place where changes to the data occurred (Parsipenny, United States), constituted the place where the offence took place.

The Court held that the real-time nature of the communication link between Levin and the Citibank computer meant that Levin's keystrokes were actually occurring on the Citibank computer.

It is thus important that in order to resolve disputes related to jurisdiction, the issue of territoriality and nationality must be replaced by a much broader criteria embracing principles of reasonableness and fairness to accommodate overlapping or conflicting interests of States, in the spirit of universal jurisdiction.2

*****

1 [1996] All ER 350, HL.