CHAPTER II
CONCEPTUAL ANALYSIS
OF CYBER CRIME
CHAPTER II

CONCEPTUAL ANALYSIS OF CYBER CRIME

Presently in India as well as in the world the computers have become an integral part of the fast developing society. The computers are being used in various aspects such as in Banking, Manufacturing, health care, defense, insurance, scientific research, strategic policy making, law enforcement etc.¹

If we think presently about the society without the computer everything seems to be impossible for example Railway Ticketing system. Airline Ticketing as well as traffic control, Electricity bill, Telephone Bill office works etc, all are seems to be impossible without the computer. Computers with the aid of the Internet have today become the most dominant medium of communication, information, commerce and entertainment. The internet is like life in the real world being extended and carried on in another medium that cuts across boundaries space, time, nationality, citizenship, jurisdiction, sex, sexual orientation, and age. Every coin has two side likewise, internet having all benefits of anonymity, a liability, and convenience has become as appropriate place for pensions interested in making are of the net for illegal gainful purpose, either monetary or otherwise.²

Internet has transformed the world into a Global Information Village. Internet has also made this world a virtual sleeper’s global market place. History is a witness to the most fact that all the technological inventions have been put to as much destructive use as constructive one. Information technologies are no different, while good people are using Information technology for finding better alternatives which can improve the quality of human life while bad elements are using it for harming individuals, cheating others of their hard earned money, subverting and defrauding the business and to hide their crimes.3

2.0 History and development of Internet

Internet has transformed the world into a Global Information Village. Internet made this world a virtual sleepless global market place. Internet is a global network of computer.4

Internet and online services, sometimes called as “new media” services as in many respects similar to the traditional media as it also includes production oriented material such as music, audio, video, graphics, text and games. It works in communication forms also likewise messaging, chatting, video conferencing etc.

The internet’s roots can be traced from 1950’s. In 1957 the Soviet Union launched the first Satellite, Sputnik I, triggering US president Dwight

---

3 Cloniel Prasad, R.S, Cybercrime-An Introduction. Hydrabad, ICFAI Publications, ed.1
2004, p-II.
4 Ibid; p-I.
Eisenhower to creating the ARPA agency to arms race. So, the evolution of internet can be said to be started with the use of ARPANET sponsored by US military, which was set up in 1969.\(^5\)

The first communication touch place between research Center at the University of California at Los Angles and the Stanford research Institute. The ARPANET was as joint venture of Massachusetts Institute of Technology and the American Department of Defense Advance Research Project Administration as a source to establish continued communication between remote computer resources in the event of war. The communication links were confined to military, defense contractors and university laboratories involved in defense related research.

In early 1970’s further innovations took place, such as electronic mail possibilities has grown. During this period other network equivalent to ARPANET being established such as the United Kingdom’s Joint Academic Network (JANET) and the United States National Science foundation Network (NSENET).\(^6\)

In the year 1990 the US authorities released ARPANET and transferred it to National Science Foundation (NSFNET).

---


In the year 1993 Time Berners-Lee’s he is the person who developed the World Wide Web (www) in the European Laboratory for particle physics (CERN).

The first commercial browser, Netscape, was launched in 1994, with Microsoft launching its own Internet explorer the preceding year. So, there browsers made Internet access possible from personal computers. From the year mid 1990’s various commercial Internet Services Providers (ISP) entered the market and offered the Internet connection through conventional telephone line.7

On 24 October, 1955 Federal Networking Council (NFNC) unanimously passed a resolution defining the term Internet. This definition was developed in consolation with members of the Internet and Intellectual property Rights communities. The term internet defined as: “Internet” refers to the global information system that (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extension or follow-ons (ii) is able to support communications using the transmission control protocol/internet protocol (TCP/IP) suit or its subsequent extensions/follow ons, and or other IP compatible protocols and (iii) provides,

7 Ibid, pp.7&8.
uses or makes accessible either publicly or privately, high level service layered on the communications and related infrastructure described herein.\(^8\)

2.1 Evolution Nature and scope of Cyber Crime

Cybercrime is the deadliest epidemic confronting our planet in this millennium. At present when everything from microwave ovens and refrigerators to nuclear power plants are being run or computers cybercrime has assumed rather sister implication.\(^9\) It has raised its head as multi headed hydra. Where if one is being cut other and newer kinds of crimes are appear or develop suddenly cyber crime can involve criminal activities that are traditional in nature, such as theft, fraud forgery, defamation and mischief. The above of computer has also providing an scope of new age crime such as hacking, web defacement cyber stalking, web jading etc.

Cyber crime is a twentieth century foetus of technological development, now which grown up like as epidemic and has become uncontrollable in the twenty-first century.\(^10\)

The first cybercrime took place in the year 1820. Joseph-Marie Jacquard, a textile unmanufactured in France produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquardi employed that their traditional employment and


\(^9\) Nagpal, Rohas, *Cybercrime and corporate liability*, Delhi, CCH India, 2008 p. 166.

livelihood were being threatened. They committed the acts of sabotage to discharge Jacquard from further use of the new technology. So, this is the first-recorded cyber crime.\footnote{Supra 9.}

2.2 Categories of cyber crime

There are different categories of cyber crimes they are as follows:

2.2.1 Data Crime

a. Data Interception

An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. However, in all variants of this attack, and distinguishing this attack from other data collection methods, the attacker is not the intended recipient of the data stream. Unlike some other data leakage attacks, the attacker is observing explicit data channels (e.g. network traffic) and reading the content. This differs from attacks that collect more
qualitative information, such as communication volume, not explicitly communicated via a data stream.\textsuperscript{12}

b. Data Modification

Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites.\textsuperscript{13}

In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. An example of this is changing the dollar amount of a banking transaction from $100 to $10,000.

In a replay attack, an entire set of valid data is repeatedly interjected onto the network. An example would be to repeat, one thousand times, a valid $100 bank account transfer transaction.

c. Data Theft

Term used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other


personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law.\textsuperscript{14}

2.2.2 Network Crime

a. Network Interferences

Network Interfering with the functioning of a computer Network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing Network data.

b. Network Sabotage

'Network Sabotage' or incompetent managers trying to do the jobs of the people they normally are in charge of network. It could be the above alone, or a combination of things. But if Verizon is using the help the children, hindering first responders line then they might be using network problems as an excuse to get the federal government to intervene in the interest of public safety. Of course if the federal government forces these people back to work what is the purpose of unions and strikes anyway.\textsuperscript{15}

2.2.3 Access Crime

a. Unauthorized Access


"Unauthorized Access" is an insider’s view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality.\textsuperscript{16}

b. Virus Dissemination

Malicious software that attaches itself to other software like virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are examples of malicious software that destroys the system of the victim.\textsuperscript{17}

2.2.4 Related Crimes

a. Aiding and Abetting Cyber Crimes

There are three elements to most aiding and abetting charges against an individual. The first is that another person committed the crime. Second, the individual being charged had knowledge of the crime or the principals' intent. Third, the individual provided some form of assistance to the principal. An accessory in legal terms is typically defined as a person who assists in the commission of a crime committed by another or others. In most cases, a person charged with aiding and abetting or accessory has knowledge of the crime either before or after its occurrence. A person who is aware of a crime before it


occurs, and who gives some form of aid to those committing the crime, is known in legal terms as an "accessory before the fact." He or she may assist through advice, actions, or monetary support. A person who is unaware of the crime before it takes place, but who helps in the aftermath of the crime, is referred to as an "accessory after the fact".  

b. Computer-Related Forgery and Fraud: Computer forgery and computer-related fraud constitute computer-related offenses.

c. Content-Related Crimes: Cyber sex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses.

The total cost to pay by victims against these attacks is in millions of millions Dollar per year which is a significant amount to change the state of under-developed or under-developed countries to developed countries. Some of the facts related to cyber crimes can be significantly marked by the information provided by a US base news agency are:

- Research study has found that one in five online consumers in the US have been victims of cybercrime in the last two years.


• RSA, the security division of EMC have released their Quarterly Security Statistics Review concerning identity theft online, phishing and malware, data breaches and data loss.

• The review found that 23 percent of people worldwide will fall for spear phishing attacks, while web pages are infected on average every 4.5 seconds.

• In Australia, cybercrime costs businesses more than $600 million a year, while in the US, one in five online consumers have been victims of cybercrime in the last two years, equating to $8 billion.

• The review also found that consumers are increasingly concerned about their safety online. The Identity Theft Resource Centre, 2009 Consumer Awareness Survey in the US found that 85 percent of respondents expressed concern about the safety of sending information over the Internet, while 59 percent expressed a need for improvement in the protection of the data they submit over websites.

• Reported cases of spam, hacking and fraud have multiplied 50-fold from 2004 to 2007, it claims.\(^20\)

• One recent report ranked India in 2008 as the fourteenth country in the world hosting phishing websites.\(^21\) Additionally, the booming of

call centers in India has generated a niche for cyber criminal activity in harvesting data, the report maintained.

- The words of Prasun Sonwalkar\textsuperscript{22} reflects the threat of cyber crime in India, India is fast emerging as a major hub of cyber crime as recession is driving computer-literate criminals to electronic scams, claimed a study by researchers at the University of Brighton. Titled 'Crime Online: cyber crime and Illegal Innovation', the study states that cyber crime in India, China, Russia and Brazil is a cause of "particular concern" and that there has been a "leap in cyber crime" in India in recent years, partly fuelled by the large number of call centers.

From Crime Desk of UK\textsuperscript{23} said that online fraud is worth around £50 billion a year worldwide, with criminal gangs increasingly using the latest technology to commit crimes, provoking the Association of Police Officers to state in the FT that "the police are being left behind by sophisticated gangs".

Computer spam refers to unsolicited commercial advertisements distributed online via e-mail, which can sometimes carry viruses and other programs that harm computers. For the year to date, the UAB Spam Data Mine


has reviewed millions of spam e-mails and successfully connected the hundreds of thousands of advertised Web sites in the spam to 69,117 unique hosting domains, Warner said. Of the total reviewed domains, 48,552 (70%), had Internet domains or addresses that ended in the Chinese country code ".cn". Additionally, 48,331 (70%) of the sites were hosted on Chinese computers.\(^{24}\)

Many of the African countries are lack of the cyber policies and laws (many articles and news are available at\(^{25}\) in this support). Due to this a cyber criminal may escape even then that is caught. Countries like Kenya, Nigeria, Tunisia, Tanzania etc. are almost free from the cyber laws and policies.

The above coated text are only some of the examples related to US, Europe, Asia and Africa to show the horrible situation of cyber crimes. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, in the current manuscript a systematic understanding of cyber crimes and their impacts over society with the future trends of cyber crimes are explained.

2.3 Classification of Cybercrime:

Broadly speaking, the cyber crimes refer to all activities done with criminal intent in cyber space. They can be divided into three categories:

2.3.1 Cyber Crime against person;

---

\(^{24}\) Newswise (2009), China Linked to 70 Percent of World’s Spam, Says Computer Forensics Expert, Available at: http://www.newswise.com/articles/view/553655/, (Visited on December 10, 2010).

2.3.2 Cyber Crime against property (against business and Non business organization);

2.3.3 Cyber Crime against Government.

2.3.1 Cyber Crime Against Person

The first category of cyber crimes committed against person include various like transmission of child-pornography, sexual harassment of any one with the use of a computer, such and e-mail and cyber stalking. Any unwanted contact between two people that directly or indirectly communicates a threat or place the victim in fear can be considered stalking. The Trafficking, distribution, posting and dissemination of absence material including pornography, indecent exposure and child pornography constitutes one of the most important cyber crimes know today. The potential harm of such a crime to humanity can hardly be over stated.26

Similarly the cyber harassment is a distinct Cyber crime various kinds of harassment can and does occur in cyber space or through the cyberspace. The internet is a wonderful place to work, play and no less than a mirror of the real world and that means it also contains electronic versions of real life problems, stalking and harassment are problems that many also occur on the internet which will be discussed in full fudge in preceding chapter.

2.3.2 Cyber Crime against property

The second category of cyber crime is that of cyber crimes against all types of property. These crimes include hacking, unauthorized use of computer and network resources, and cracking. Hacking involves breaking into someone else's computer system, often on a network, or intentionally breaching computer security. Virus is a computer programme that can reproduce itself and cause destruction of data contamination. Copyright protects creative or artistic works. You should only copy or copyrighted work with the copyright owner's permission. Infringement, imitation, cyber fraud, cyber squatting, and trafficking in or using a domain name with bad-faith intent to profit are among the gravest cyber crimes known till date. It is a dreadful feeling to know that someone has broken into your computer systems without your knowledge and consent, tampered with precious confidential data, and information. Coupled with this, the reality is that no computer system in the world is hacking proof. So, it is unanimously agreed that any and every system in the world can be hacked.

2.3.3 Cyber Crime against Government

Cyber terrorism could be defined as the premeditated, politically attack against information system, computer programs, and data to deny service or
acquire information with the intent to disrupt the political, social or physical infrastructure of a target resulting in violence against public.\textsuperscript{27}

During 1998 LTTE Liberation Tigers of Tamil Elam, attacked a large number of Sri Lanka Embassy's computer system all over the world by releasing 800 e-mails to each embassy, everyday, over a two week period with the messages, we are internet black tigers and we are using this to disrupt your communications: This is first known attack by terrorists against a country's computer system. The chapter IV of the thesis is wholly related with this particular aspect.

2.4 Cyber Crime and Organized Crime

The internet revolution has transformed the society in general and the commercial world in particular\textsuperscript{28} While commercial dealing is rampant on the internet due to its reach worldwide in low cost. So organized crime also found the new opportunities and benefits on internet that are very useful for furthering the criminal activities organized criminal groups are gradually moving from traditional criminal activities to more rewarding and less risky operations in cyberspace. Some traditional criminal groups are seeking the co-operation of e-criminals with the necessary technical skills, newer types of criminal networks operating in the area of e-crime have already emerged.\textsuperscript{29}


\textsuperscript{28} Ibid, p-15.

\textsuperscript{29} Dr. Tropina, Tatiana, available at: http://www. freedomfromfear magazine.org, (Visited on August 2, 2010).
According to Phil Williams of University of Pittsburgh, organized crime is primarily about the pursuit of profit and can be understood in Clausewitzian terms as a continuation of business by criminal means. The objective of organized crime is also to earn profits through businesses, but the only difference is that the business activity or means of contracting the business may be illegal.\(^3\)

Criminal organizations are constantly on the lookout for new opportunities as well as new ways of keeping themselves safe and away from the law enforcing authorities. Internet offers a number of services for the common man and criminals could abuse many of those services to their advantage. Internet is most inexplicable and realizable Id. These attributes attract the criminals as well as also help them in speeding up their activities. The structure of these criminal organization is different from traditional organized crime organization. Criminal activities are usually conducted within multi-skilled, multifaceted virtual criminal networks centered on online meetings. These networks are structured on "Stand alone" basis, as members rarely meet each other in person and sometimes do not even have a virtual contact with other colleagues. This sophisticated structure, together with access to the core operations granted only to trusted associates, prevents organized cybercrimes groups from being detected and infiltrated by law enforcement.

2.5 Cyber Crime and Legislation of Nations

To meet the challenges posed by new kinds of crime made possible by computer technology including telecommunication, many of the countries largely industrialized and some of those which are moving towards industrialization have in part few years reviews their respective domestic criminal laws from the point of adaptation, further development and supplementation so as to prevent computer related crime. A number of countries have already introduced more or less extensive amendments by adding new statutes in their substantive criminal law.\[^{31}\]

According to McConnell International some counties laws are substantially or particularly updated laws, while some others have no updated law. So, here in figure 1, I classified there laws in two categories i.e. 1- updated law (Substantially or partially) 1 and 2- No updated laws.

List of Countries with Updated Laws (Partially or substantially) and no Updated Laws

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Updated Law (Substantially Partially)</th>
<th>S. No.</th>
<th>No Updated Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Australia</td>
<td>1</td>
<td>Albania</td>
</tr>
<tr>
<td>2</td>
<td>Canada</td>
<td>2</td>
<td>Bulgaria</td>
</tr>
<tr>
<td>3</td>
<td>Estonia</td>
<td>3</td>
<td>Burundi</td>
</tr>
<tr>
<td>4</td>
<td>India</td>
<td>4</td>
<td>Cuba</td>
</tr>
<tr>
<td>5</td>
<td>Japan</td>
<td>5</td>
<td>Dominican Republic</td>
</tr>
<tr>
<td>6</td>
<td>Mauritius</td>
<td>6</td>
<td>Egypt</td>
</tr>
<tr>
<td>7</td>
<td>Peru</td>
<td>7</td>
<td>Ethiopia</td>
</tr>
<tr>
<td>8</td>
<td>Philippines</td>
<td>8</td>
<td>Fiji</td>
</tr>
<tr>
<td>9</td>
<td>Tunkey</td>
<td>9</td>
<td>France</td>
</tr>
<tr>
<td>10</td>
<td>United States</td>
<td>10</td>
<td>Gambia</td>
</tr>
<tr>
<td>11</td>
<td>Brazil</td>
<td>11</td>
<td>Hungry</td>
</tr>
<tr>
<td>12</td>
<td>Chile</td>
<td>12</td>
<td>Iceland</td>
</tr>
<tr>
<td>13</td>
<td>Chines</td>
<td>13</td>
<td>Iran</td>
</tr>
<tr>
<td>14</td>
<td>Czech Republic</td>
<td>14</td>
<td>Italy</td>
</tr>
<tr>
<td>15</td>
<td>Denmark</td>
<td>15</td>
<td>Jordan</td>
</tr>
<tr>
<td>16</td>
<td>Malaysia</td>
<td>16</td>
<td>Kazakhstan</td>
</tr>
<tr>
<td>17</td>
<td>Poland</td>
<td>17</td>
<td>Latina</td>
</tr>
<tr>
<td>18</td>
<td>Spain</td>
<td>18</td>
<td>Lebanon</td>
</tr>
<tr>
<td>19</td>
<td>United Kingdom</td>
<td>19</td>
<td>Lesotho</td>
</tr>
<tr>
<td>20</td>
<td></td>
<td>20</td>
<td>Malta</td>
</tr>
<tr>
<td>21</td>
<td></td>
<td>21</td>
<td>Moldova</td>
</tr>
<tr>
<td>22</td>
<td></td>
<td>22</td>
<td>Morocco</td>
</tr>
<tr>
<td>23</td>
<td></td>
<td>23</td>
<td>New Zealand</td>
</tr>
<tr>
<td>24</td>
<td></td>
<td>24</td>
<td>Microglia</td>
</tr>
<tr>
<td>25</td>
<td></td>
<td>25</td>
<td>Nigeria</td>
</tr>
<tr>
<td>26</td>
<td></td>
<td>26</td>
<td>Norway</td>
</tr>
<tr>
<td>27</td>
<td></td>
<td>27</td>
<td>Romania</td>
</tr>
<tr>
<td>28</td>
<td></td>
<td>28</td>
<td>South Africa</td>
</tr>
<tr>
<td>29</td>
<td></td>
<td>29</td>
<td>Sudan</td>
</tr>
<tr>
<td>30</td>
<td></td>
<td>30</td>
<td>Vietnam</td>
</tr>
<tr>
<td>31</td>
<td></td>
<td>31</td>
<td>Yugoslavia</td>
</tr>
<tr>
<td>32</td>
<td></td>
<td>32</td>
<td>Zambia</td>
</tr>
<tr>
<td>33</td>
<td></td>
<td>33</td>
<td>Zimbabwe</td>
</tr>
</tbody>
</table>
Figure 1, which listed the countries, who are updated their legislation for combating Cyber Crime. The list of countries as mentioned in figure 1 is the initiative of McConnell International who surveyed its global network of information technology, Cyber Security Laws the around the world.

McConnell International asked the countries to send their respective legislation is respect of the Cyber Crime. Over fifty countries responded through sending their piece of legislation, on that basis figure 1 divided into two column i.e. (i) updated laws (substantially or partially), and (2) No updated laws so, in column (1) the list of Countries comprises both substantially as well as partially, in this column from Sl. No. 1 to 10 are the countries which have fully updated laws and rest of the countries have partially updated laws.

There is no uniformity in the legislation among the nations. So, here it will be better to chart another figure which depicts which types of cyber crimes have been addressed through these updated legislations of the nationa.

Figure 2, countries with updated law from McConnell international. As, I have discussed earlier that there is uniformity among the statutes of different countries. So, the different features of the statues in different countries are as:

Australia: Has included offence related to computers in the Australian crime Act. The penalty for damaging data in

---

computers is imprisonment up to 10 yrs and for unlawful data in computers imprisonment from 6 months to 3 years.

**Canada:** Has named three Computer Crimes (a) Possession of devices to obtain unauthorized telephone facilities; (b) unauthorized access to computer; (c) Committing mischief with data. The imprisonment varies from 2 years to upto 10 years depending the nature of the crime.

**Germany:** Classified Compute Crime Like data spying, computer fraud, alternation of data and computer sabotage. The punishment varies from 2 years to 5 years depending upon the nature of crime.

**Singapore:** Computer Misuse Act refers to unauthorized access to computer system with intent to commit or facilitate commission of offence, unauthorized modification of computer material etc. Punishment is Imprisonment from 2 yrs to up to 5 yrs with fine.

**Japan:** Amended its penal code which, refer to activities as computer crime. Electronic record wrongfully made by a public servant false entry in permit license or passport, interference with business by destruction or damage of computerized data, interference with computer and destruction of private and public documents.

**United Kingdom:** Computer Misuse Act included unauthorized access to computer material or system and unauthorized access with
intent to commit or facilitate commission of further offences as the computer crimes. The punishment is imprisonment from 6 months to up to 5 yrs with five.


These acts classified computer crimes, as (a) willful unauthorized access of computer related to national defense or foreign relation (b) intentional access of computer without authorization to obtain financial information, (c) unauthorized access of computer of a government department or an agency, (d)

\(^{33}\) *Aligarh Law Journal 1999-2000*, p.34.
unauthorized access of computer federal, internet with intent to defraud, (c) knowingly causing transmission of data/programme to damage a computer network or deny use of computer, network etc, (f) knowingly causing transmission of data/programme with risk that transmission will damage a computer network, data or program or without or dent use of computer, network etc. and (g) unauthorized access of computer with intent to defraud.  

2.6 Cyber crime and Indian Position

The first cyber crime took place as early as in the year 1820. The crimes have however gained momentum in India only in the recent past. As an upshot, the Indian Parliament gave effect to a resolution of the General Assembly of the United Nations for adoption of a Model Law on Electronic Commerce. The consequence was the passing of Information Technology Act 2000. The Act aims to regulate and legalize E-Commerce and take cognizance of offences arising there from.

The Information Technology Act deals with the following cyber crimes along with others:

2.6.1 Tampering with computer source documents

A person who knowingly or intentionally, conceals (hides or keeps secret), destroys (demolishes or reduces), alters (change in characteristics) or causes another to conceal, destroy, and alter any computer source code used for a

34 Ibid.
computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law is punishable. For instance, hiding the C.D.ROM in which the source code files are stored, making a C File into a CPP File or removing the read only attributes of a file.

2.6.2 Hacking

Hacking is usually understood to be the unauthorized access of a computer system and networks. Originally, the term "hacker" describes any amateur computer programmer who discovered ways to make software run more efficiently. Hackers usually "hack" on a problem until they find a solution, and keep trying to make their equipment work in new and more efficient ways. A hacker can be a Code Hacker, Cracker or a Cyber Punk.

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 means is said to commit hacking.

Vinod Kaushik and Ors. v. Madhvika Joshi and Ors.\(^{35}\)

The main issue in this case is whether accessing a husband's and father-in-law's email account without their permission amounts to 'unauthorized access'. In this case, the first respondent had accessed the email account of her husband and

\(^{35}\) Before Sh. Rajesh Aggarwal, Adjudicating Officer, Information Technology Act, 2000, Government of Maharashtra, At Mantralaya, Mumbai-400032, Complaint No.2 of 2010. available at: http://docs.google.com/open?id=0B8vVw0jzMxE0Y2EyM2I1ZTQtNmQ3Yy00MDhjLTg z... (visited on January 23, 2012).
father in law, in order to acquire evidence in a Dowry harassment case. The Adjudicating Officer held that accessing an e-mail account without authorization amounts to a contravention of section 43 of the Information Technology Act 2000. There was no compensation awarded to the complainant as the respondent had only submitted the information so obtained to the police and the court. The Adjudicating Officer, however ordered the first respondent to pay a fine of Rs. 100, as she was held to be in contravention of Section 66-C (identity theft and dishonest use of the password of any other person) of the IT Act 2000.

It is to be noted that there cannot be any defense of bonafide intention, in case of violation of privacy by accessing e-mail accounts without the consent of the user. It will be still construed as 'unauthorized access'. It is also interesting to note that the adjudicating officer relied on the reasoning that the information procured by the 'unauthorized access' was only disclosed to the Court and the police, therefore the respondent is not liable to pay any compensation to the complainant. However, Section 43 of the IT Act 2000 deals with the penalty and compensation for an 'unauthorized access' to any computer or computer system or computer network. It may be said there is a lacuna in the reasoning of the Adjudicating Officer. It also gives rise to the question whether a person is not liable to pay compensation under Section 43 if the information obtained by 'unauthorized access' is only disclosed before competent authorities such as police or court. The 'unauthorized access' of an e-
mail account by dishonest use of password of any other person also amounts to violation of privacy. It is covered under Section 66C of the IT Act 2000.

2.6.3 Publishing of information, which is obscene in electronic form

A person who publishes or transmits or causes to be published in the electronic form, any material which is lascivious, or if its effect is such as to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it, is liable to punishment. The important ingredients of such an offence are publishing (make generally known or issue copies for sale to public), or transmitting (transfer or be a medium for), or causing to be published (to produced the effect of publishing), pornographic material in the electronic form.

2.6.4 Child Pornography

Child Pornography is a part of cyber pornography but it is such a grave offence that it is individually also recognized as a cyber crime. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The Internet is very fast becoming a household commodity in India. Its explosion has made the children a viable victim to the cyber crime. As more homes have access to Internet, more children would be using the Internet and more are the chances of falling victim to the aggression of pedophiles. The pedophiles use their false identity to trap children and even contact them in various chat rooms where they befriend them and gain personal information from the innocent preys. They even start contacting children on
their e-mail addresses. These pedophiles drag children to the net for the purpose of sexual assault or so as to use them as a sex object. Chapter III of the thesis discuss all issues related with the pornography and child pornography.

2.6.5 Accessing protected system

Any unauthorized person who secures access or attempts to secure access to a protected system is liable to be punished with imprisonment and may also be liable to fine.

2.6.6 Breach of confidentiality and privacy

Any person who, secures access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned or discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be liable to be punished under the Information Technology Act.

K.L.D Nagasree v. Government of India, represented by its Secretary, Ministry of Home Affairs and Ors.\(^\text{36}\)

A writ petition was filed in the Andhra Pradesh High Court challenging the order of the respondent under Section 5(2) of the Indian Telegraph Act 1885. The respondent gave the order to intercept messages from the mobile phone of the petitioner. The Court examined the procedural safeguards that are in place in case with respect to an order of interception of communication. These

\(^{36}\) AIR2007AP102, (Andhra Pradesh High Court).
Conceptual Analysis of Cyber Crime

safeguards are enshrined in Rule 419-A of the Indian Telegraph Rules 1951 pursuant to the guidelines laid down by the Supreme Court in the case of *PUCL v. Union of India*.\(^{37}\) The Court, while considering the impugned order, decided that the order did not record the reasons for the interception. The Court also discovered that the Review Committee constituted under Rule 419-A (8) had without any reason delayed the review of the impugned order. The Court also laid down in this case that the procedural inconsistencies render any recorded evidence inadmissible in Court. The Court also observed that the enforcement agencies were not observing the correct procedure for interception of communications under Section 5(2) of the Indian Telegraph Act. It ordered that any such recording should be destroyed.

It is one of the few instances where the Court has gone on record to say that the enforcement agencies are not following the procedure established by law, with regard to giving out of orders for interception of communication under Section 5(2) of the India Telegraph Act 1885. Disregard to procedural safeguard by the enforcement agency amounts to a gross violation of right to privacy envisaged under Article 21 of the Constitution of India.

*Rayala M. Bhuvaneswari v. Nagaphanender Rayala*\(^{38}\)

This case came up before the Andhra Pradesh High Court under a revision petition for a voice test of a tape recording. In this case, the Court discovered

\(^{37}\) *AIR 2004 SC 1442.*

\(^{38}\) *AIR 2008 AP 98* (Andhra Pradesh High Court).
that the husband had tape-recorded a telephone conversation of his wife with her friends and parents, without her consent. Subsequently, he had been using this as evidence in the divorce case between the parties. The Court, at the very outset, held that there had been clear violation of privacy of the wife by her husband. It also cited the compilation of Federal Law on "Covertly Recording Telephone Conversation", which makes it unlawful to record telephone conversation except in one-party consent cases. One-party consent cases are those cases where the person can record their own telephone conversation without the consent or knowledge of the other party. But in this case no consent had been given by either party of the telephone conversation.

The Court held that the act of the husband was illegal and unconstitutional, and infringed upon the privacy of the wife. Even if the tapes were accurate, they could not be admissible as evidence.

This is one of cases where the Court has acknowledged that the protection of right to privacy under Article 21 of the Constitution of India is not only enforceable against the State but also against individuals. The Court also held that any recording which infringes upon the right to privacy of an innocent person cannot be admitted as evidence in a court of law.

*Nirav Navin Bhai Shah and Ors. v. State of Gujarat and Another*39

The appellants were accused of hacking into the computer system of the complainant and stealing important data. The main issue was whether criminal proceedings can be quashed on the ground that the parties have reached an amicable settlement. The Court decided that if the 'entire' dispute has been amicably settled then the Court shall quash criminal proceeding to that effect.

In this case the appellants were charged under section 66 and 72 of the Information Technology Act 2000 along with other offences under the Indian Penal Code 1860. The complainant argued before the Court that the criminal proceeding should be quashed as the dispute is civil in nature. The Court rejected the contention, while stating that the offense cannot be viewed as a civil dispute because offenses under section 66 and 72 of the Information Technology Act 2000 are offenses against the society and cannot be condoned. The Court however, quashed the FIR based on the reasoning that there was an amicable settlement of the 'entire dispute'. It also took into consideration that if criminal proceedings were continued, a miscarriage of justice would be the result.

The Gujarat High Court observed that violation of privacy and hacking are offenses against the society and cannot be condoned or treated as a civil dispute. However, if the parties agree to a settlement of the 'entire' dispute then the Court may allow such settlement in the interest of justice.

2.7 Cyber crimes other than those mentioned under the IT Act

2.7.1 Cyber Stalking
Although there is no universally accepted definition of cyber Stalking, it is generally defined as the repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using Internet services. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harms to the victim. It all depends on the course of conduct of the stalker.

2.7.2 Cybersquatting

Cybersquatting is the obtaining of a domain name in order to seek payment from the owner of the trademark, (including business name, trade name, or brand name), and may include typosquatting (where one letter is different).

A trademark owner can prevail in a cybersquatting action by showing that the defendant, in bad faith and with intent to profit, registered a domain name consisting of the plaintiff's distinctive trademark. Factors to determine whether bad faith exists are the extent to which the domain name contains the registrant's legal name, prior use of the domain name in connection with the sale of goods and services, intent to divert customers from one site to another and use of false registration information and the registrant's offer to sell the domain name back to the trademark owner for more than out-of-pocket expenses.
2.7.3 Data Diddling

This kind of an attack involves altering the raw data just before a computer processes it and then changing it back after the processing is completed.

The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipts and bank remittances.

2.7.4 Cyber Defamation

Any derogatory statement, which is designed to injure a person's business or reputation, constitutes cyber defamation. Defamation can be accomplished as libel or slander. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person’s friends.

2.7.5 Trojan Attack

A Trojan, the program is aptly called an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.
2.7.6 Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. It is very difficult to control such attacks. For e.g. across the country students buy forged mark sheets for heavy sums to deposit in college.

2.7.7 Financial crimes

This would include cheating, credit card frauds, money laundering etc. such crimes are punishable under both IPC and IT Act. A leading Bank in India was cheated to the extent of 1.39 crores due to misappropriation of funds by manipulation of computer records regarding debit and credit accounts.

2.7.8 Internet time theft

This con notes the usage by an unauthorized person of the Internet hours paid for by another person. This kind of cyber crime was unheard until the victim reported it. This offence is usually covered under IPC and the Indian Telegraph Act.

2.7.9 Virus/worm attack

Virus is a program that attaches itself to a computer or a file and then circulates to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make
functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

2.7.10 E-mail spoofing

It is a kind of e-mail that appears to originate from one source although it has actually been sent from another source. Such kind of crime can be done for reasons like defaming a person or for monetary gain etc. E.g. if A sends email to B’s friend containing ill about him by spoofing B’s email address, this could result in ending of relations between B and his friends.

2.7.11 Email bombing

Email bombing means sending large amount of mails to the victims as a result of which their account or mail server crashes. The victims of email bombing can vary from individuals to companies and even the email service provider.

2.7.12 Salami attack

This is basically related to finance and therefore the main victims of this crime are the financial institutions. This attack has a unique quality that the alteration is so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a programme whereby a meager sum of Rs 3 is deducted from customers account. Such a small amount will not be noticeable at all.
2.7.13 Web Jacking

This term has been taken from the word hijacking. Once a website is web jacked the owner of the site loses all control over it. The person gaining such kind of an access is called a hacker who may even alter or destroy any information on the site.

2.7.14 Crackers

These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.

2.7.15 Hackers

These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.

2.7.16 Pranksters

These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.

2.7.18 Career criminals

These individuals earn part or all of their income from crime, although they Malcontents,\textsuperscript{40} addicts, and irrational and incompetent people: "These

\textsuperscript{40} One who rebels against the established system.
individuals extend from the mentally ill do not necessarily engage in crime as a full-time occupation. Some have a job, earn a little and steal a little, then move on to another job to repeat the process. In some cases they conspire with others or work within organized gangs such as the Mafia. The greatest organized crime threat comes from groups in Russia, Italy, and Asia. "The FBI reported in 1995 that there were more than 30 Russian gangs operating in the United States. According to the FBI, many of these unsavory alliances use advanced information technology and encrypted communications to elude capture".  

2.7.19 Cyber terrorists

There are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of like-minded Internet users who crash a website by flooding it with traffic. No matter how harmless it may seem, it is still illegal to those addicted to drugs, alcohol, competition, or attention from others, to the criminally negligent. Earlier when IT Act enacted in 2000 the punishment was silent but after amendment in 2008 the punishment has been prescribed.

2.7.20 Cyber bulls

Cyber bullying is any harassment that occurs via the Internet. Vicious forum posts, name calling in chat rooms, posting fake profiles on web sites, and mean or cruel email messages are ways of cyber bullying.

---

2.7.21 Salami attackers

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

The following is a table in brief showing the various offences under the Information Technology Act, 2000 together with their respective punishments:

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Offence</th>
<th>Punishment</th>
<th>After amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Tampering with computer source document</td>
<td>Imprisonment up to 3 years, Fine up to 2 lakh rupees.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Hacking with computer system</td>
<td>- DO -</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Failure to comply with direction of the controller</td>
<td>- DO -</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Breach of confidentiality or privacy</td>
<td>Imprisonment up to 2 years, Fine up to one lakh rupees.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Publishing false digital certificate</td>
<td>- DO -</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Publishing digital certificate for fraudulent purposes</td>
<td>- DO -</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Misrepresentation or suppression of material facts</td>
<td>- DO -</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Failure to assist to decrypt information</td>
<td>Imprisonment up to 7 years</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>Securing access to protected systems</td>
<td>Imprisonment up to 10 years and fine</td>
<td></td>
</tr>
</tbody>
</table>
2.8 Challenges posed by cyber crime

As the cyber law is growing, so are the new forms and manifestations of cyber crimes. Russia, China and Brazil are world leaders in cyber crime and India is fast emerging as a major hub of cyber crime in spite of enacting IT Act, 2000 to regulate and control cyber crimes. This situation raises apprehensions and concerns about the efficacy of our cyber law in dealing with cyber crimes.

It can’t be disputed that Information Technology Act, 2000 though provides certain kinds of protections but doesn’t cover all the spheres of the I.T where the protection must be provided. The offences defined in the IT Act, 2000 are by no means exhaustive. However, the drafting of the relevant provisions of the IT Act, 2000 makes it appear as if the offences detailed therein are the only cyber offences possible and existing. It does not cove various kinds of cyber crimes and Internet related crimes. These Include Theft of Internet hours, Cyber theft , Cyber stalking, Cyber harassment, Cyber defamation, Cyber fraud, Misuse of credit card numbers, Chat room
abuse. Even issues like cyber war against India or cyber terrorism against India have not been incorporated into the IT Act yet.

Copyright and trade mark violations do occur on the net but Copyright Act 1976, or Trade Mark Act 1994 are silent on that which specifically deals with the issue. There is no enforcement machinery to ensure the protection of domain names on net. Transmission of e-cash and transactions online are not given protection under Negotiable Instrument Act, 1881. Online privacy is not protected only Section 43 (penalty for damage to computer or computer system) and 72 (Breach of confidentiality or privacy) talks about it in some extent but doesn’t hinder the violations caused in the cyberspace.

One of the important issues relating to taking legal action against cyber criminals is jurisdictional issue. The whole trouble with internet jurisdiction is the presence of multiple parties in various parts of the world who have only a virtual nexus with each other. Then if one party wants to sue the other, where can he sue? Traditional requirements generally encompass two areas—firstly, the place where the defendant resides, or secondly where the cause of action arises. In the context of Internet, both these are difficult to establish with any certainty. Issues of this nature have contributed to the complete confusion and contradictions that plague judicial decisions in the area of internet jurisdiction. Further compounding the problem is the issue that a particular act in one national jurisdiction is legal and not barred by law, but the same activity may be considered as illegal and barred by law in another country. In such a case
Governments can take action against cyber criminals only when there is a valid extradition treaty between the respective countries.

The most serious concern about the Indian Cyber law relates to its implementation. The IT Act, 2000 does not lay down parameters for its implementation. When internet penetration in India is extremely low and government and police officials, in general are not very computer savvy, the new Indian cyber law raises more questions than it answers. A recent survey indicates that for every 500 cyber crime incidents that take place, only 50 are reported to the police and out of that only one is actually registered. These figures indicate how difficult it is to convince the police to register a cyber crime. The establishment of cyber crime cells in different parts of the country was expected to boost cyber crime reporting and prosecution. However, these cells haven't quite kept up with expectations.\textsuperscript{42}

Even the basic 'e-mail tracking' procedures sometimes pose as a big challenge before the law enforcement agencies in India. It would be a 'dangerous trend' to follow to arrest or detain suspects on the basis of mere 'IP addresses' or 'e-mail addresses' as they are very easy to be spoofed and forged. It requires tremendous cyber forensics expertise to correctly trace the culprit. The recent incidents of wrongfully arresting innocent persons and imprisoning them for a considerable time on the basis of spoofed e-mail addresses is a glaring example of faulty and novice cyber forensics application

\textsuperscript{42} http://www.isrj.net/PublishArticles/289.aspx, (Visited on September 29, 2012).
in India. There is every need to strengthen cyber forensic systems to prevent the harassment of innocent people at the hands of overzealous police officers.

The real issue is how to prevent cybercrime. For this, there is need to raise the probability of apprehension and conviction. The absolutely poor rate of cyber crime conviction in the country has also not helped the cause of regulating cyber crime. There has only been few cyber crime convictions in the whole country, which can be counted on the fingers. The challenge in cyber crime cases includes getting evidence that will stand scrutiny in a foreign court. For this India needs total international cooperation with specialized agencies of different countries.

According to CID Detective Inspector M D Sharath, study on cyber crimes shows there is no tendency of the crimes slowing down. The 2011 research reports highlighted the new advanced threats and an increased of sophistication in the attacks.\footnote{http://thehackersmedia.blogspot.ro/2012/09/cyber-crime-biggest-challenge-to-cops.html, (Visited on October 28, 2012).}

India is projected to be the third largest internet user base in the world in 2013 with over 120 million internet users in India. Electronic payments in India account for 35.3 per cent of the local transactions in terms of volume and 88.3 per cent in terms of value. India also has the world's second largest mobile phone user base with 894 million users as on December 2011. However, the NCRB Cyber Crime Statistics reveal that 1791 cyber crime cases are registered under the IT Act 2008. There is an increase of 85.4 per cent cases
over 2010. As many as 422 cases are registered under IPC and 1184 persons have been arrested, he said.  

Case Laws

Cases filed under the Information Technology Act 2000

Radiological and Imaging Association v. Union of India

A circular was issued by the District Magistrate of Kolhapur, requiring sonologists and radiologists to install silent observers (SIOB) in all sonography machines and to submit an online form F under the Pre-Conception and Pre-Natal Diagnostic Technique Rules 2003. The circular was challenged under Article 226 of the Constitution on the ground that it violates the right to privacy of the patients.

The Petitioner argued, inter alia, that there would be a violation Section 72 of the Information Technology Act 2000 if the impugned circular was implemented. The Court did not find any merit in this claim and clarified that Section 72 of the IT Act was not applicable in the case as it only deals with 'any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder'.

In this case the information was not considered to be obtained under the IT Act 2000 but under the Pre-Conception and Pre-Natal Diagnostic Technique Rules 2003. The Court also observed that the allegation of invasion of privacy


45 2011(113) Bom. LR3107 (Bombay High Court).
due to the silent observer is far fetched as the images stored in the silent observer are not transmitted online to any server and stay stored in the sonography machine. There are also safeguards in place, including those requiring the removal of the silent observer device, and requiring the appropriate authority to enter a user name and password, which are under the control of Collector.

The Court held that right to privacy is not absolute and is subject to restrictions on the grounds of public interest. It also held that there are enough procedural safeguards to protect the privacy of the patients.

*Shankara Shekhar Mishra v. Ajay Gupta* 46

The plaintiff bought a laptop for the purpose of web design and other functions. He also stored personal data on his laptop, including family photographs and bank details. The defendant, who was also involved in similar business of web design, barged into the premises of the plaintiff and snatched his laptop, which contained confidential and personal information. The plaintiff filed for a permanent injunction for the rendition of accounts, delivery of the infringing material and damages.

The Court took into consideration that there was ample amount of personal information on the laptop, which also contained vital financial data. The court asserted that the privacy of the plaintiff had already been invaded. The defendant had no right to transfer the information to any other person and

---

46 2011VIIIAD(Delhi) 139 (Delhi High Court).
the plaintiff was entitled to an injunction restraining the defendant to further transfer the information. The Court also noted that the plaintiff had gone though mental trauma and would be in constant fear that the data stored by him on the laptop may be misused by the defendant. The Court reiterated the value of privacy and stated that monetary compensation is widely recognized as the remedy to violation of right to privacy against State or individual. In its final order, the Court passed a permanent injunction restraining the defendant from infringing the copyright of the plaintiff in the "literary works" authored by the plaintiff, and restrained the defendant from disclosing the information of the defendant and his family stored on the laptop snatched to any person. In this case it is interesting to note that the Court also took into account the invasion of privacy along with the theft of laptop while deciding on the quantum of the compensation.

**Interception of Communication**

*State of Maharashtra v. Bharat Shanti Lal Shah and Ors.*

The legislative competence of the State to enact Sections 13-16 of the Maharashtra Control of Organized Crime Act 1999 (MCOCA) was challenged. The court, while deciding on the constitutional validity of the impugned sections, which deal with the interception of wireless, electronic or oral communication, observed that although the interception of communications is an invasion of an individual's right to privacy, the right to privacy is not absolute, thus the court must see that the procedure itself be fair, just, and

47 (2008) 13 SCC 5 (Supreme Court).
reasonable.\(^{48}\) It was also observed by the Court that MCOCA provides for sufficient procedural safeguards to avoid invasion of privacy, and hence the impugned sections are constitutionally valid and do not infringe upon right to privacy.

This case lays down the limits to the exercise of the right to privacy. It also reiterates that the State has the legislative competence to enact laws that may curtail the right to privacy of an individual. However, such laws should lay down fair, just and reasonable procedure with respect to the issuance and implementation of orders of interception of conversation or communication.

_Amar Singh v. Union of India\(^{49}\)

In this case the petitioner is a political leader of the opposition party. At the outset the petitioner had filed a writ petition before the Supreme Court under Article 32 of the Constitution, seeking to protect his right to privacy under Article 21. The petitioner in his petition mentioned that Respondent No. 7 (Indian National Congress) pressurized the Government of India and the Government of the National Capital Region of Delhi to monitor and record the phone conversations of the petitioner. The petitioner has also sued in court asking the Court to direct telecom service providers to reveal the details as to the order of interception.

The Court dismissed the writ petition, on the ground that such a writ petition is frivolous, because of the change in the facts in the subsequent


\(^{49}\) (2011) 7 SCC 69 (Supreme Court).
affidavits filed by the petitioner. In considering the facts of the case the
Supreme Court said that it is the duty of the service provider to give assistance
to the law enforcement agencies, as and when required. Any violation of such a
condition may lead to heavy imposition of penalty on the service provider.
However, the Court observed that, "[i]n view of the public nature of the
function of a service provider, it is inherent in its duty to act carefully and with
a sense of responsibility." It further laid down that the service provider while
acting on orders of interception should simultaneously verify the authenticity of
the same from the author of the document.

In order to avoid forgery of orders of interception of communication,
which may lead gross violation of privacy, the Supreme Court laid down the
guidelines to be followed by the telecom service providers while assisting law
enforcement agencies with intercepting communication.

Phishing

*NASSCOM v. Ajay Sood*\(^5^0\)

The plaintiff filed the suit asking for a permanent injunction, restraining the
defendants or any other person from acting under their authority to send and
circulate fraudulent e-mails that appear to be sent by the plaintiff due to the use
of the trademark 'NASSCOM' or any other mark which is confusingly similar.
It is the first judgment in India that recognized phishing. The Court observed
that there is no law in India that deals with phishing. However, within the

\(^5^0\) 2005 (30) PTC 437.
purview of the existing laws, it could be considered to be a form of misrepresentation, passing off and defamation.