Chapter 10

Judicial approach and legal control
Chapter 10

JUDICIAL APPROACH AND LEGAL CONTROL

10.1 Introduction

In India, adversarial trial system is followed in the criminal justice dispensing mechanism. The system is typically reflecting the colonial impact where the power has been conferred on the prosecution and the accused has been guarded with rights. The adversarial model is based on the principle of ‘innocent, unless proved guilty’ and prosecution has to prove the case beyond doubt in order to punish accuse. The role of the judge in this system is quite neutral and both prosecution and accuse are the party to contest on the case. Prosecution is responsible for bringing all the fact before the court and prove it beyond reasonable doubt. Thus right from the beginning of filing of first information report (F.I.R.), the investigation machinery put into action and start investigation and settling charges against the accuse. As soon as the investigation with respect to crime is completed by the police officer, the charge sheet is filed in the court which is beginning of trial process. During this stage, the both the prosecution lawyer and defence lawyer contest their plea and try to prove and disprove the allegations levelled against. The judge has to decide the issue on the ground of the evidences and documents placed before him and during trial both parties try to convince the judge about their plea. Thus judge is quite neutral in this case and generally burden of proof lies on the prosecution to prove the charges beyond reasonable doubt.

Thus the above system as we have seen show quite passive role for judiciary to play in the criminal justice system and major active participation to investigate and impose criminal liability on accuse is done by the investigation machineries.

10.1.1 Judiciary plays less important role in investigation

Therefore, in adversarial model, the judicial play the passive role and benefit of doubt is always given to accuse. The model heavily favour and strengthen the position of accuse which resulted into the downfall of conviction rate. This also leads into vesting of the control mechanism into investigating machineries which are having equipped with the power. The power to arrest, seizure, taking good behaviour bond, making interrogation, seizure of passport, asking the accuse to have periodical attendance at police station, power to take into custody on any doubt etc., etc.
The direct involvement of judicial into the matter to decide issues and their presence in the case appear very late on the scene. And even at the time of trial and argument, Judge remain neutral and both the contesting party i.e. prosecution and defence lawyer argue their case and exchange charges, allegations, facts, and issues. However, hardly, in any case judicial take the whole responsibility in their hands to find out the truth and make justice. However, no doubt, that sometime judiciary also plays role to keep judicial surveillance during investigation also. In D.K. Basu v State of West Bengal, it is the judiciary, who has given clear-cut guidelines to the police departments.

In short, the adversarial system of criminal justice shows the sign of passive role of judiciary and active role of investigation mechanism.

10.1.2 The Cyber-criminality in adversarial model of criminal justice

Thus scrutinising the presence of adversarial model in India and probably response of Indian judicial towards the Cyber-criminal pose several serious challenges raising major crises to deal with Cyber criminality. Again we are aware that in India, everything is depended upon the effectiveness of investigation mechanism and failure on their part may weaken the case of prosecution which directly benefited to accuse. Therefore if investigation mechanism fail short on their expectations to prove their case beyond reasonable doubt in the court room and the existing situation in which the judiciary play passive role make the case of Cyber criminality very difficult and again it will definitely reflected into the downfall of conviction rates. The downfall of conviction rates in Cyber criminality definitely exposes the loopholes of Judicial and investigative mechanism which would not be the happy situation from the angle of maintenance of law and order in Cyber space.

10.1.3 The crises of India Judicial System

Though common man still has faith in judiciary and solely feels protected that judiciary bring justice for him. Therefore, though justice delivering is complex phenomenon and all the governmental wings are involve in the process indirectly by way of 'distributive justice' and directly by way of 'particularly justice', people always thinks that it is Judiciary of the country which is primarily responsible for the proper

---

1 1996 (1) SCALE. See also, Ashok K. Johar Vs. State of U.P. AIR 1987 the Basu's case is an outcome of W.P. (Crl.) No. 592 of 1987 in the present case.
administration of Justice. Therefore, judicial approach towards the issues in legal disputes is very essential and of prime importance.

Today though Indian judiciary is posing various crises, which is not the focus point of discussion here, it is essential to know the judicial approach on various issues involved in the Cyber space and comparative analysis of those issues in other part of the globe.

In this part, the main focus has been shifted to know the judicial approach on the various issues involved in the Cyber space like, pornography, online gambling, et al., so that to understand it in comprehensive way.

10.2 The Judicial response to the incidences of Cyber crimes

10.2.1 Judicial response with respect to 'Unauthorised Access'

Unauthorised access to any computer system is punishable at law. Accessing the computer system without prior and proper permission of its owner is always attracted civil and criminal liability.

Under the Information Technology Act, 2000, the illegal access or unauthorised access deserved civil and criminal liability of the intruder. Section 43 of the act prescribes the penalty for damage to computer, computer system. If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network accesses or secures access to such computer, computer system or computer network shall be liable to pay damages by way of compensation not exceeding one crores rupees to the person so affected.\(^2\) The word access means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network.\(^3\) The Information Technology Act, 2000 also define word 'Computer',\(^4\) 'Computer Network',\(^5\) 'Computer System'.\(^6\) At the same time Section 65 and Section 66 of Information Technology Act, 2000 also prescribe punishment if any person tampers with the computer source documents or hacking with computer system.\(^7\) Thus whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly

---

\(^2\) Section 43 (a) of Information Technology Act, 2000.
\(^3\) See Definitional clause Section 2 (a) of Information Technology Act, 2000.
\(^4\) Section 2 (i) of Information Technology Act, 2000.
\(^5\) Section 2 (j) of Information Technology Act, 2000.
\(^6\) Section 2 (l) of Information Technology Act, 2000.
\(^7\) See, Section 65 & Section 66 of Information Technology Act, 2000. Chapter - XI 'Offences'.
causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system of computer network, when the computer 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.  

Again 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 the means, commits hacking.  

And 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.  

Thus, unauthorised access is crime under the Information Technology Act, 2000 and attracts both civil and criminal liability on the culprit. The Judicial response to the 'unauthorised access' can be discussed with following cases.

In Briggs v. State of Maryland the Court held that the statute of the state of Maryland that criminalizes unauthorized access to computers "was intended to prohibit use of computers by those not authorized to do so in the first place, and may not be used to criminalize the activities of employees who use employers' computer systems beyond the scope of their authority to do so".

Thus, even though the person is authorised to use the system of his employer, the scope of using the system has been limited by the nature and scope of the work assigned to the concerned employees by the employers. And it is a criminal activity of employees who use employers' computer systems beyond the scope of their authority to do so.

In Scott Moulton and Network Installation Computer Services, Inc. v. VC the Court held that the plaintiff's act of conducting an unauthorized port scan and throughput test of defendant's servers does not constitute a violation of

---

8 Section 65 of Information Technology Act, 2000.
9 Section 66 (1) of Information Technology Act, 2000.
10 Section 66 (2) of Information Technology Act, 2000.
11 348 Md. 470 (1998) [USA]
either the Georgia Computer Systems Protection Act or the Computer Fraud and Abuse Act.\textsuperscript{14}

In \textit{United States v. Rice}\textsuperscript{15} dependent was an IRS agent whose long time friend was under investigation for drug dealing. At the request of his friend, Rice tried to find on the computer of IRS whether his friend was under investigation by the IRS. Rice was not the member of the team, which was assigned the job of investigation, he therefore, made an unauthorised access or exceeded his authorised access. He also went to the IRS investigator to see what the codes on the print out meant and told his friend the meaning of the codes and the investigator's name. This fraud of Rice, however, did not cause any pecuniary loss but involved unauthorised access and unauthorised disclosure of confidential information. Rice was convicted by a Jury of computer fraud for accessing the computer system of a Government agency without authority and his conviction was latter on confirmed.

Similarly if a person provides any assistance to facilitate access to any other person without the permission of the owner or the in charge of a computer, computer system or computer network in contravention of the provisions of the IT Act, 2000, rules, regulations made there under, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Thus the test applied here that if the ultimate intention of the person is to benefit the computer system by conducting unauthorized port scan cannot be treated as unauthorised access to the computer system.

In \textit{Regan Gerard Gilmour v. Director of Public Prosecutions}\textsuperscript{16}, the accused was a public servant employed as an Administrative Services Officer Grade 3 within the Debt Management Section of the Australian Taxation Office in its Relief Section. The Relief Section considers written applications by taxpayers for relief from payment of income tax.

Upon receipt of an application the Relief Section prepares a submission, which objectively sets out the application and attaches relevant documents but makes no recommendation as to whether or not relief should be granted and the

\textsuperscript{14} http://www.asianlaws.org/cyberlaw/library/cc/cee_caselaw.htm Accessed on 05 June 2004, 23:35:16
\textsuperscript{15} 1992 U.S. App. LEXIS 9562 (4th Cir. May 4, 1992). Quoted from Farooq (Dr.) Ahmed, 'Cyber Law in India (Law on Internet)', Pioneer Books, Delhi, P. 319
\textsuperscript{16} (Commonwealth) No. 60488/95 In The Supreme Court Of New South Wales [Australia]
submission is forwarded together with the application to an appropriate person. This appropriate person then determines whether or not relief should be granted.

Following the determination of an application, the accused was required to insert data into a computer system called the Compact Computer System, which operated, only in the Debt Management Section. This data was eventually entered on the taxpayer's general file held by the Australian Tax Office.

The accused had no authority to grant relief. For the purpose of carrying out the duties of his employment, he had access to the computer by entering his user ID and password. His duties included the entry of various codes into the computer.

He was permitted by his employer to enter relief code "43" only where relief had been granted.

The computer system had the capacity to be programmed to restrict the insertion of data and to beep and display the words "no right of access" if insertion was attempted contrary to the restriction. The computer was not so programmed to restrict entry of relief code "43" by the appellant.

In 19 cases no grant of relief had been made and the accused knew this to be the case. Accordingly, the appellant was not permitted by his employer to enter relief code "43" in these cases. However, in all the 19 cases, the accused inserted data, relief code "43", in the computer indicating that relief had been granted when this was not the case. The computer received this data in each case.

There was no financial gain to the accused in taking this course. He did so because of a desire to expedite the process, a heavy workload and concern about suggested inconsistencies in determinations of applications for relief.

The Court was required to determine whether the accused had "authority" to insert data in a Commonwealth computer for the purpose of section 76C of the Crimes Act 1914 when

i. the computer would physically accept his insertion of data, but

ii. the accused was not permitted by his employer to insert the relevant data, relief code "43", in the computer without
specific permission given by the employer prior to the insertion and such permission was not given in these cases”.

As per section 76C of the Crimes Act 1914, "A person who intentionally and without authority or lawful excuse: (a) destroys, erases or alters data (Data" is defined by section 76A as including information, a computer program or part of a computer program) stored in, or inserts data into, a Commonwealth computer….. is guilty of an offence".

The Court held that a person commits an offence under this section if he lacks the authority to insert the particular information into a computer, notwithstanding that he has general authority to insert other information into such computer.

The Court further held that an entry intentionally made without lawful excuse and known to be false is made without lawful authority.17

In Director of Public Prosecutions v Murdoch18 In this case, the court held that section 76 C of the Crimes Act 1914 does not distinguish between what are colloquially known as “hackers”….. and persons who have some authority of some kind to enter the computer system. Rather the section invites attention to whether the particular entry or gaining access to the computer system was with or without lawful authority.

The Court held that where the question is whether the entry was with permission, it would be important to identify the entry and to determine whether that entry was within the scope of the permission that had been given. If the permission was not subject to some express or implied limitation, which excluded the entry from its scope, then the entry will be with lawful justification but if the permission was subject to an actual express or implied limitation, which excluded the actual entry, made, then the entry will be "without lawful authority to do so".

The Court also held that in the case of an employee the question would be whether that employee had authority to affect the entry with which he stands charged. If he has a general and unlimited permission to enter the system then no offence is proved. If however there are limits upon the permission given to him to enter that system, it will be necessary to ask, was the entry within the scope of that permission? If

18 (1993) 1 VR 406 [Australia]
it was, then no offence was committed; if it was not, then he has entered the system without lawful authority to do so. ¹⁹

**Some other famous cases on Unauthorized access:**

**The United States v Kevin David Mitnick**

Kevin Mitnick has been described as the "most famous computer hacker of all." His crimes included the hacking and theft of countless computer files that stored valuable information for the corporations involved. He also stole thousands of personal credit card numbers and would relax by reading people's personal e-mail. Although his crimes are considered major in the eyes of the computer world, their non-violent nature makes it hard for the rest of the world to be overly concerned with them. His motives, although mischievous, never involved harm in the traditional sense of crime. This is due to the fact that he never used the files or credit card numbers for personal gain. There are problems involved in defining the cat and mouse games of these new age pranksters as crime.

The nature of Mitnick's crimes invades on the privacy of individuals, corporations, and made everyone subject to the possibility of becoming a victim. Even though these threats are very real, the perception of these actions as crimes is still difficult to comprehend. As more people become victims, however, the reality of the dangers of cyber crime will begin to actualize their potential. In order to combat further breaches of privacy in the Mitnick case, the FBI and one of Mitnick's victims Tsutomu Shimomura combined their forces to track down an individual that seemed untraceable. This mission entailed an extensive "electronic manhunt." Ironically this manhunt used many of the same techniques that Mitnick used as a hacker. Tracing Mitnick through the different files and corporations he attacked, Shimomura would re-attack the same institutions in an attempt to find the patterns and traceable likenesses in Mitnick's style. For two long months the authorities followed Mitnick's moves and finally captured him on February 15th 1995.

In August 1999, Kevin was sentenced for certain admitted violations of his supervised release and for possession of unauthorized access codes. The court imposed a sentence of nearly four years in prison. Since Kevin has been in custody since his arrest in February 1995, this sentence has been satisfied. On

January 21 2003, Kevin Mitnik was released from the conditions of supervised release, which had prohibited him from using a computer and from acting as consultant or advisor in any computer-related matters.\footnote{http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16}

***CISCO System v Geoffrey Osowski and Wilson Tang***

Former Cisco Systems, Inc., accountants Geoffrey Osowski and Wilson Tang were each sentenced to 34 months in prison for exceeding their authorized access to the computer systems of Cisco Systems in order to illegally issue almost $8 million in Cisco stock to themselves. The two were charged with one count of conspiracy to commit computer and wire fraud in violation of Title 18, United States Code, Section 371, one count of computer fraud in violation of Title 18, United States Code, Section 1030(a)(4), and three counts of wire fraud in violation of Title 18, United States Code, Section 1343.

In pleading guilty, Mr. Osowski and Mr. Tang admitted that between October 2000 and March 27, 2001, they participated together in a scheme to defraud Cisco Systems in order to obtain Cisco stock that they were not authorized to obtain. As part of the scheme, they exceeded their authorized access to computer systems at Cisco in order to access a computer system used by the company to manage stock option disbursements, used that access to identify control numbers to track authorized stock option disbursements, created forged forms purporting to authorize disbursements of stock, faxed the forged requests to the company responsible for controlling and issuing shares of Cisco Systems stock, and directed that stock be placed in their personal brokerage accounts.

The two defendants admitted that the first time that they did this, in December 2000, they caused 97,750 shares of Cisco stock to be placed in two separate Merrill Lynch accounts, with 58,250 of the shares deposited in an account set up by Mr. Osowski and 39,500 shares deposited in an account set up by Mr. Tang. In February 2001, they caused two additional transfers of stock, in amounts of 67,500 shares and 65,300 shares, to be transferred to brokerage accounts in their names. The total value of the Cisco stock that they took on these three occasions (at the time that they transferred the stock) was approximately $7,868,637.
Judge sentenced the defendants each to 34 months in federal prison, restitution of $7,868,637, and a three-year period of supervised release. The defendants have begun serving their sentences on January 8, 2002.21

10.2.2 Judicial response with respect to e-mail related offences

In United States v. Kammersell22 The Court found that federal interstate jurisdiction was proper where defendant sent a threatening email via AOL, an interstate service, even though the message was sent from and received in the same state.

The Court held that federal laws prohibiting transmission in interstate commerce of communications containing threats applied, because the e-mail was sent via a commercial online service and routed outside the state before reaching its final destination within the state.23

Thus it should be noted down that the traditional territorial jurisdiction of Criminal court does not effectively works in Cyber space and even the foreign court adopted the approach that though physical presence of person or system may lies in any jurisdiction, the court through which the networking, server or services are provided can also be the ground for entertaining the jurisdiction of the court and culprit can not avoid taking plea that the computer system or actual commission of crime took place outside the jurisdiction of court.

In another case United States v. Machado24 the accused was convicted in violation of federal hate-crime law for sending threatening email to Asian students at University of California at Irvine based on race/ethnicity. The accused stated that the emails were sent idly and without intention to act on the threats.

In State of Washington v. Townsend25 a Washington Appellate Court affirmed a conviction for second-degree rape of a child. The defendant appealed the lower court’s decision to admit into evidence copies of email messages between himself and a police officer posing as a 13 year old girl.

22 1998 U.S. Dist. LEXIS 8716 (D. Utah 1998) [USA]
23 The 10th Circuit Court of Appeals affirmed this decision (See 196 F.3d 1137 (10th Cir. Utah 1999) [USA]. For more details see, http://www.asianlaws.org/cyberlaw/library/ce/ce_caselaw.htm Accessed on 05 June 2004, 23:35:16
24 C.D. Cal. 2/10/98 [USA]
25 No. 19304-7-III (Wash. Ct. App. 2001) [USA]
The defendant argued that the email messages were copied in violation of the Washington Privacy Act, which prohibits the "copying of private communications transmitted by telephone, telegraph, radio, or other device...."

The court held that email by its nature must be recorded, and an email user impliedly consents to the copying by the act of using email. Accordingly, the court affirmed the lower court’s decision to admit the email messages.26

Thus though e-mail is private communication and Right to privacy prohibit the disclosure of private communication, however, such e-mails by its nature can be ground for convicting the accuse. In the present case, e-mail was considered as on of the document by the court to convict the accused. The same principle may be adopted in India to prosecute the accused who threaten greed, pose different identity, or ask illegal money from the person. Incidentally it should be noted down that recently the Delhi based NRI Mr. Sanjay Kapoor, the husband of famous actress Karishma Kapoor was threaten by one of the person by sending e-mail from Cyber cafe of Mumbai asking 50 lakhs rupees. There was a pending litigation going on between Sanjay Kapoor and Karishma Kapoor. Thus, same test can be applied to punish the accused.

In America Online Inc. v. National Health Care Discount, Inc27 the court denied plaintiff AOL’s motion for summary judgment seeking to hold defendant liable for violations, inter alia, of the Computer Fraud and Abuse Act, the Virginia Computer Crimes Act, and common law trespass to chattels, as a result of the transmission of unsolicited bulk e-mail advertising defendant’s products to AOL users. The court reached this conclusion because, based on the record before it, it could not determine whether the parties who sent the e-mail in question were defendant’s agents, acting under its control, or independent contractors.28

Thus before prosecuting the person for sending illegal and abused e-mails, the connection between defendant and e-mail should be established. In absence of such connection, defendant cannot be held liable to be prosecuted.

10.2.3 Judicial response on Defamation

27 2000 U.S. Dist. Lexis 17055 (N.D. Iowa, September 29, 2000 [USA]
The law gives protection to a man's reputation, which to some is dearer than life itself. Love of reputation inspires people to do great things, acquire fame and name, which is the mainspring of life in every walk of life. The aim of the law of defamation is to protect one's reputation, honour and dignity in the society. A person needs protection of his reputation, honour, integrity and character as much as the right to the enjoyment of property, health, personal safety, liberty and a number of other privileges.  

Defamation is the publication of a statement which reflects on a person's reputation and tends to lower him in the estimation of right thinking members of society generally or tends to make them shun or avoid him.  

The defamation in India attracts both civil and criminal liability. Person is entitled to get relief in the form of unliquidated damages for defamation under Law of Tort. if he proved that defendant cause defamation to his reputation. At the same time the person can also be held criminally liable under Section 499 of Indian Penal Code, 1860.

So far as the defamation in electronic form is concern, there is not problem in either in prosecuting the accused person or taking civil relief from him. Because Section 29A of Indian Penal Code, 1860 consider any document in electronic form with the definition of 'document' and it can be brought in the court of law to support the case.

In Anderson v New York Telephone Co the plaintiff was a bishop. A person by the name of Jackson broadcast a programme on radio urging the listeners to call up two telephone numbers.

'A person calling these numbers would hear accusations against plaintiff involving him in all sorts of scurrilous activities not the least of which was illegitimately fathering children by women and girls in the church. Jackson's telephones were attached to equipment leased to Jackson by defendant. This equipment contained the recorded messages which would automatically play upon activation of the telephone by a caller.  

---

30 Winfield and Jolowicz on Tort, 10th Ed. By W.V.H. Roger (1984), P. 293. See also Ashok Kumar v. Radha Kant, AIR 1967 Cal 178.
31 Ins. by Information Technology Act, 2000 [21 of 2000], Sec. 91 and Sch.1, (w.e.f. 17.10.2000)
32 (1974) 35 NY 2d 746 [USA]
The Court held that

"...the telephone company's role is merely passive and no different from any company which leases equipment to another for the latter's use... In order to be deemed to have published a libel a defendant must have had a direct hand in disseminating the material whether authored by another, or not... It could not be said, for example, that International Business Machines, Inc., even if it had notice, would be liable were one of its leased typewriters used to publish a libel. Neither would it be said that the Xerox Corporation, even if it had notice, could be held responsible were one of its leased photocopy machines used to multiply a libel many times."33

Thus the ratio of the case is the person can be held liable for the defamatory material though in electronic form. But intermediary like telephone company, Internet Service Provider, cannot not be held liable, in general, because hardly these intermediary have had a direct hand in disseminating the material.

In Cubby Inc v CompuServe Inc34 action was brought against computer Service Company for its alleged libel, business disparagement, and unfair competition. On company's motion for summary judgment, the District Court, Leisure, J., held that: (1) computer service company that provided its subscribers with access to electronic library of news publications put together by independent third party and loaded onto company's computer banks was mere "distributor" of information, which could not be held liable for defamatory statements made in news publications without showing that it knew or had reason to know of defamation.

'CompuServe develops and provides computer-related products and services, including CompuServe Information Service ("CIS"), an on-line general information service or "electronic library" that subscribers may access from a personal computer or terminal. Subscribers to CIS pay a membership fee and online time usage fees, in return for which they have access to the thousands of information sources available on CIS. Subscribers may also obtain access to over 150 special interest "forums," which are comprised of electronic bulletin boards, interactive online conferences, and 349 topical databases.

34 (1991) 776 F Supp 135 [USA]
One forum available is the Journalism Forum, which focuses on the journalism industry. Cameron Communications, Inc. ("CCI"), which is independent of CompuServe, has contracted to "manage, review, create, delete, edit and otherwise control the contents" of the Journalism Forum "in accordance with editorial and technical standards and conventions of style as established by CompuServe".

"New York courts have long held that vendors and distributors of defamatory publications are not liable if they neither know nor have reason to know of the defamatory. "The requirement that a distributor must have knowledge of the contents of a publication before liability can be imposed for distributing that publication is deeply rooted in the First Amendment, made applicable to the states through the Fourteenth Amendment"

CompuServe's CIS product is in essence an electronic, for-profit library that carries a vast number of publications and collects usage and membership fees from its subscribers in return for access to the publications.

CompuServe and companies like it are at the forefront of the information industry revolution. High technology has markedly increased the speed with which information is gathered and processed: it is now possible for an individual with a personal computer, a modem, and telephone line to have instantaneous access to thousands of news publications from across the world.

While CompuServe may decline to carry a given publication altogether, in reality, once it does decide to carry a publication, it will have little or no editorial control over that publication's contents. This is especially so when CompuServe carries the publication as part of a forum that is managed by a company unrelated to CompuServe.... CompuServe has no more editorial control over such a publication than does a public library, book store, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so.

"First Amendment guarantees have long been recognized as protecting distributors or publications ... Obviously, the national distributor of hundreds of periodicals has no duty to monitor each issue of every periodical it distributes.
Such a rule would be an impermissible burden on the First Amendment. "... Technology is rapidly transforming the information industry.

A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, a bookstore, or newsstand would impose an undue burden on the free flow of information. Given the relevant First Amendment considerations, the appropriate standard of liability to be applied to CompuServe is whether it knew or had reason to know of the allegedly defamatory Rumorville statements.\(^{35}\)

This is famous case which settles various issues pertaining to the incidences of defamation online. The case ca be treated as best guideline for the Indian incidences also.

In another case from Norway, Norway v. Tvedt\(^{36}\) the accused was the founder of a far right group in Norway. He was convicted for posting racist material that mixed neo-Nazism, racial hatred, and religion, on a website. He was held responsible for the material despite the fact that it was posted on a server that was based in the United States.\(^{37}\)

Again in Stratton Oakmont v Prodigy\(^{38}\) the Court held that 'A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, bookstore, or newsstand would impose an undue burden on the free flow of information.'

The Court held that computer bulletin boards should generally be regarded in the same context as bookstores, libraries and network affiliates. The Court held that in this case, because of PRODIGY’s own policies, technology and staffing decisions, the scenario had been altered and the Court held that PRODIGY was a publisher.\(^{39}\)

\(^{35}\) http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16

\(^{36}\) Ask and Baerum District Court (Norway, 2002) [NORWAY]


\(^{38}\) (1995) NY Misc Lexis 229 [USA]

In *Zeran v America Online Inc*\(^{40}\) the Court held that a federal immunity was granted to any cause of action that would make service providers liable for information originating with a third-party user of the service and that lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are barred.

*Lunney v Prodigy Services Co*\(^{41}\) has factual similarity to the present case.

### 10.2.4 Judicial response in the cases of Computer fraud

Though the incidents of computer fraud in India is very less as compare to developed nations, but looking to the percentage of increase in the computer and automation process, the day will come when the incidences of computer fraud will be on its peak. Therefore, it is essential to see what are the judicial responses in other nations with respect to computer fraud, and guiding ratio developed in the said cases. Particularly in trade and commerce and intellectual property area, the computer fraud incidents are very high. And as Indian is presently think tank for the world computer technology especially in software industry; it is essential to discuss some of the cases on this subject.

In *FTC v. Craig Lee Hare*\(^{42}\) in this case the action was for deceptive trade practices arising from on-line "auction" offering sale of computer products that were never delivered.

The Defendant pleaded guilty to wire fraud and was sentenced to six months home detention, three years probation and ordered to pay restitution of over $22,000. He was also barred for life from conducting Internet commerce. \(^{43}\)

In another case *United States v. Middleton*\(^{44}\) the court held that the term "individual" as used in the Computer Fraud and Abuse Act, is not confined to natural persons, but extends to business entities, and hence damage to an ISP-victim was encompassed under the statute.\(^{45}\)

---

\(^{40}\) 120 F.3d 327 [USA]

\(^{41}\) 250 AD 2d 230

\(^{42}\) S.D. Fla. 4/1998 [USA]

\(^{43}\) http://www.asianlaws.org/cyberlaw/library/cc/ce_caselaw.htm Accessed on 05 June 2004, 23:35:16

\(^{44}\) 35 F. Supp. 2d 1189 (N.D. Cal. 1999) [USA]

\(^{45}\) http://www.asianlaws.org/cyberlaw/library/cc/ce_caselaw.htm Accessed on 05 June 2004, 23:35:16
Thus with respect to computer fraud the term is widely interpreted by the court where the incidences of abuse also extended to the business entities, and hence damage to an ISP-victim was encompassed under the statute. Now, ISP or business entities can also be within the coverage area of the court so far as computer fraud is concerned.

In United States v. Hoke\(^{46}\) a suit was filed against Gary Hoke for disseminating misinformation on a counterfeit Bloomberg News Service Web page regarding an alleged merger between his employer PairGain Technology, Inc. and ECI Telecom, Ltd.

Initial investigation by the FBI revealed that Hoke might have used services of Angelfire.com\(^{47}\) to host the page and Hotmail email service.

Hoke was traced by IP addresses from these services. Hoke, pled guilty and was sentenced to five months of home detention, five years probation, and restitution of $93,086.77.\(^{48}\)

In another case United States v. Pirello\(^{49}\) the Ninth Circuit ruled on the application of the US Sentencing Commission Guidelines (USSG) about a defendant fraudulently selling computers online.

The defendant Pirello placed four advertisements on Internet classified-ads websites, soliciting buyers for computers. Pirello received three orders, deposited the money in his personal bank account, and never delivered computers.

The court determined that USSG 2F1.1(b)(3), which instructs courts to enhance a sentence by two levels if the offense was committed through "mass-marketing," applied to Pirello's fraudulent Internet advertisements. The court held that the use of the Internet website to solicit orders for non-existent computers violated the USSG and affirmed the lower court's enhancement of Pirello's sentence.\(^{50}\)

In Kennison v Daire\(^{51}\) in this case, the accused held an automatic teller machine (ATM) card which enabled him to withdraw funds from his account from

---

\(^{46}\) Magistrate No. 99-889M (C.D. Cal. 4/14/99) [USA]


\(^{48}\) http://www.asianlaws.org/cyberlaw/library/co/ce_case04.htm Accessed on 05 June 2004, 23:35:16

\(^{49}\) 255 F.3d 728 (9th Cir. 2001) [USA]

\(^{50}\) http://www.asianlaws.org/cyberlaw/library/co/ce_case04.htm Accessed on 05 June 2004, 23:35:16

\(^{51}\) (1986) 169 CLR 129 - [AUSTRALIA]
a certain bank by inserting the card and keying in his personal identification number; but it was a condition of his use of the card that the customer's account could be drawn against to the extent of the funds available in that account.

The accused closed the account but subsequently used the card to withdraw funds. It was held that it was not sufficient that the bank had programmed the computer to permit the withdrawal, as the bank consented to the withdrawal by the cardholder who presented his personal identification number only if the cardholder had an account, which was current, and accordingly the appellant was guilty of larceny.

The Court further held that "The fact that the Bank programmed the machine in a way that facilitated the commission of a fraud by a person holding a card did not mean that the Bank consented to the withdrawal of money by a person who had no account with the Bank. It is not suggested that any person, having the authority of the Bank to consent to the particular transaction, did so. The machine could not give the Bank's consent in fact and there is no principle of law that requires it to be treated as though it were a person with authority to decide and consent". 52

Thus ATM and other computer related fraud used to happened in India. As most of the banks are providing the ATM facilities to their customers and as the ATM facility greatly benefited to subscriber, as it is convenient to have money round the clock, the use of ATM credit and debit cards is growing day by day. Under this backdrop, these cases are very important and can be taken to develop the judicial strategy to prosecute the misdemeanor.

10.2.5 Judicial response to the pornographic and obscene literature in electronic form

The pornography, as discussed in Chapter IV 53 of this research writing, is vary dangerous, and pornography in electronic form is worse than worst. As it provide a visual presentation, easy access, difficult to detect make is more dangerous than in printed form. The various issues that involve in pornographic and obscene literature and its effect on its audience may corrupt, and if the viewer

53 See Chapter IV- 'Forms and varieties of Cyber-crimes and related phenomenon' of this research paper. Point 4.2 Pornography and related issues.
belongs to tender age group, it cause bad effect. Here are some of the cases in
which court has responded on the pornographic and related issue.

In Davis v. Gracey, after the accused, Davis, sold obscene CD-ROMs to
an undercover officer, a warrant was obtained to search his business premises;
police officers determined pornographic CD-ROM files could be accessed through
the bulletin board and seized the computer equipment used to operate it.

Following his criminal conviction and civil forfeiture of the computer
equipment in state court proceedings, Davis, his related businesses, and several
users of email on his bulletin board brought action against the officers who
executed the search, alleging that the seizure of the computer equipment and email
and software stored on the system violated constitutional and statutory provisions.

Affirming, the 10th Circuit held that the original warrant was not
unconstitutionally overbroad, and that the incidental temporary seizure of bulletin
board email users' files did not invalidate the seizure of the computer within which
they were stored. "The computer equipment was more than merely a 'container' for
the files; it was an instrumentality of the crime."

Thus to seize the all instrumentality which are incidental to cyber crime is
not unconstitutional and not illegal. In order to find out the clue it is major
source. The hard disc of the computer may contain important valuable
information regarding crime. Therefore, to have seizure to collect the evidence
alleged accused person is not illegal. However, it problem may not arise in India
because under Indian criminal system, as it reflects based on adversarial model, a
vide power has been given to police.

While dealing with the ground to consider any material obscene or
pornographic, in United States v. Thomas a Bulletin Board Service (BBS)
operator in California was arrested and convicted when pornographic materials
from their site were downloaded by a federal postal inspector in Tennessee (USA),
and materials ordered from them were delivered, violating federal obscenity laws.
Conviction and sentence were affirmed.

---

54 111 F.3d 1472 (10th Cir. 1997) [USA]
56 See Chapter V - Arrest of persons from Section 41 to 60 of Cr.P.C., 1973
57 74 F.3d 701 (6th Cir. 1996) [USA]
The Court held that GIF files are not "intangible" for purpose of federal obscenity laws; distribution of obscene materials was "knowing" even without defendants having specific knowledge of each individual transmission; obscenity may be measured by "community standard" in place where materials are received; defendants' ability to control subscriptions and access to their BBS made them liable for the downloading that occurred in Tennessee, and thus amenable to jurisdiction there. The court distinguished the subscriber-BBS from an "Internet-type" situation, in which the person posting the materials has no control over where they will be downloaded.58

Thus in this case the test of "community standard" has been applied.

In United States v. Kufrovič59 defendant, charged under 18 U.S.C. § 2422(b) and § 2423(b) with using a means of Interstate Commerce to knowingly persuade a minor to engage in sexual activity moved to dismiss, alleging that the Supreme Court's finding that portions of the Communications Decency Act were unconstitutional made Internet speech presumptively protected under the First Amendment. Because Defendant's contact with the victim had been through the Internet, it was constitutionally protected and could not be used in evidence against him, he maintained.

The court rejected the argument, holding that the statutes under which the charges were brought do not impermissibly limit speech; they criminalize the use of means of interstate commerce (such as Internet and telephone lines) for the purpose of luring a minor into sexual activity.60

Thus luring a minor into sexual activity is prime consideration and major important for the court and override the individual privilege to have speech and expression.

Similarly, M.G. v. Brian D. Travis61 the Court upheld the restriction on paroled sex offender's use of computers as within "the spirit and intent of the Legislature in enacting Megan's Law and ... within the responsibility of the Division of Parole".

59 997 F. Supp. 246 (D. Conn. 1997) [USA]
60 http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16
61 667 N.Y.S.2d 11 (1st Dep't 1997) [USA]
The Court held that "The imposition of these conditions did not violate the parolee's Double Jeopardy rights and was not arbitrary or capricious". The court held that "this condition is narrowly tailored solely to prevent petitioner from exchanging pornographic messages. Certainly, no lengthy explication is needed, in this age of 'Internet paedophilia,' to show the wisdom of this condition in preventing recidivism".

In United States v. Hookings it was held that the computer graphic interchange files (GIFs) in binary format fall within the definition of "visual depictions" as contemplated by 18 U.S.C. §§ 2252(a)(1) and (4)(B).

The fact that such files require the use of personal computer hardware and software to depict images of child pornography does not put them outside the statute, the court held, analogizing to an earlier case in which undeveloped film was also held to constitute a "visual depiction" under the statute.

Again in United States v. Simpson the court held that the Detective's affidavit describing aborted transaction negotiated in Internet chat room to exchange child pornography was sufficient to constitute probable cause in obtaining search warrant.

It should also be noted down that each time the pornographic or obscene act will be treated separately. Each incidences of visiting, downloading, viewing the porn material create separate offence each time and cannot be clubbed together. In United States v. Matthews the Court held that each transfer by email of a child pornography image is a separate offence under federal law. The Court rejected the defendant's argument that the successive email transmissions were all part of a single online "conversation".

The U.S. District Court for the District of Maryland also rejected the defendant's First Amendment defense based on the claim that he was involved in investigative journalism. The Fourth Circuit Court of Appeals affirmed this decision.

---

63 129 F.3d 1069 (9th Cir. 1997) [USA]
65 152 F.3d 1241 (10th Cir. 1998) [USA]
67 11 F. Supp. 2d 656 (D. Md. 1998) [USA]
In People v. Barrows, New York penal code law § 235.22, bars the knowing transmission of sexual materials to a minor by computer with the intent to lure the minor into sexual activity. This deed was held to, prima facie, be unconstitutional.

Analogizing to Reno v. ACLU, the Court held that the inherent vagueness of the terms in the code to describe elements of the crime would insidiously end all communication on the Internet related to sex (this would also include communication with regard to Sex education).

However, § 263.19, prohibiting "promoting an obscene sexual performance by a child" was upheld. The court distinguished the two code sections, reasoning that the upheld section was unrelated to the age of the recipient of the proscribed communication.

Another case can be quoted here on the same topic. In Germany v. CompuServe Deutschland, et al, German District Court Judge Wilhelm Hubbert convicted Felix Somm, the former head of CompuServe Germany, of child pornography for failing to block third parties' postings of pornographic pictures using CompuServe's services.

Somm received two years probation and was fined DM 100,000, despite the fact that under current German law ISPs are not held responsible for banned information on the Internet if they are unaware of the existence of the material.

The conviction was overturned on appeal. However its important and issued discuss cannot be underestimated and not far from the judicial importance.

Similarly in United States v. Whiting, appeals court held that change of definition of "visual depiction" in law banning child pornography did not violate ex post facto clause because previous definition already included data stored on computer disks, although not explicitly. Amendment made to include electronic data was a clarification rather than a substantive change.

The court struck down the attempt of an accused to take shelter of loopholes by raising the plea of constitutional bar for ex-post facto law.
In *Fedemer v. Haun*\(^{75}\) plaintiff challenged Utah's sex offender notification statute, which would make sex offender registry information available to the general public without restriction on the Internet.

The court held that the registry information posted on the Web site and available to a global audience that will have no risk of encountering the offender was not reasonably related to the non-punitive goal of preventing additional sex offences and therefore violated the Double Jeopardy and Ex Post Facto Clauses.

The court held that the statute did not violate the Equal Protection Clause because it was rationally related to the goal of guarding against sexual offences.

The Court also held that the Due Process Clause was not violated because the information to be posted is considered "non private" and therefore there is no cognizable injury to the plaintiff's reputation. The defendant, the Utah Department of Corrections, stipulated it would administer the statute in accordance with the court's decision, and therefore no order was issued.\(^{76}\)

Again in *Free Speech Coalition v. Reno*\(^{77}\) action challenging constitutionality of certain provisions of the Child Pornography Prevention Act of 1996 (CPPA), which make it illegal to post on the Internet or to show in movies, pornographic images of adults portrayed as minors.

Court held that CPPA was unconstitutional insofar that it describes as child pornography, computer images that do not involve the use of real children in their production or dissemination. Language used in the statute, prohibiting images that "appear to be a minor" and "convey the impression" of being a minor, was held to be unconstitutionally vague.

The court also noted that Congress has not articulated a compelling interest sufficient to withstand strict scrutiny. These specific provisions were struck down, but the remainder of CPPA was allowed to stand. Later, the US Supreme Court, quashing the decision, granted Certiorari.\(^{78}\)

\(^{75}\) 35 F. Supp. 852 (D. Utah 1999) [USA]
\(^{76}\) http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16
\(^{77}\) 198 F.3d 1083 (9th Cir. 1999) [USA]
\(^{78}\) http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16
In another interesting case, in *People v. Foley* the court found that the state law against knowingly transmitting sexually explicit communications to minors with intent to lure them into sexual activity was constitutional and did not violate the Commerce Clause. The court noted that the statute is no broader than necessary to achieve the purpose of preventing the sexual abuse of children.

Further in *State of New York v. BuffNet* an Internet Service Provider (ISP) pled guilty to the misdemeanour charge of knowingly providing access to child pornography. A two-year investigation found that ISP, BuffNet, knowingly hosted a child pornography newsgroup called "Pedo University". The police notified BuffNet that they were hosting illegal content, yet BuffNet failed to remove the newsgroup from its servers. Police then seized the ISP's servers. BuffNet was levied a $5000 fine, and removed the obscene content.

The case from Canada entitled, *John Robin Sharpe v. B.C.* the Supreme Court of Canada upheld a law that makes it a crime to possess child pornography.

In 1999 a trial court had struck down the law and dismissed charges against John Robin Sharpe who had been charged under the law.

In a 9-0 decision the court upheld the law, but created two exceptions. One was to protect private works of the imagination or photographic depictions of oneself, and another for those that create sexually explicit depictions of children for their own personal pleasure.

In *Regina v. Vernon Boyd Logan* The accused had pleaded guilty to possession of child pornography, contrary to section 163.1(4) of the Criminal Code.

The police had seized a variety of child pornography, mostly magazines containing photographs of physically mature teenaged boys performing sexual acts with each other, from the home of the accused. Some pictures were of pubescent boys and girls involved in sexual activities together, and a few depicted pubescent girls engaging in similar behavior.
It was not alleged that the accused had created, published, imported, distributed, or sold child pornography, or had it in his possession for any of those purposes. Moreover, there was no suggestion that the defendant has been sexually involved with children, or that the pornography had been inspired any deviant behavior by him. The accused was given an absolute discharge. The Court held that the act of merely possessing child pornography was "entirely passive". The Court held that the accused did not pose any threat to the public, as the extent of his culpability was that he had prohibited material in his possession and, presumably, read it.86

In one of the Indian case *Antony v. State of Kerala*,87 it was held that to be an obscene object, an object need not be visible to the naked eye. The fact that electrical impulses recorded on video tape are thrown on to the television screen, by electric current to the picture tube containing a cathode ray, to produce images will not make it any less visible, than any other visual object. This leads to the conclusion that the courts recognise that changes in technology could result in changes in the necessary interpretation of the law, and therefore that the words of the statue should be so construed as to make it possible to include within its ambit, images that would otherwise to be excluded from the scope of prosecution, merely because the draftsman of the legislation could not see so far as to predict a change in the prevalent technology.88

Again in *Santok Singh v. Delhi Administration*,89 it was held that,

"It is hardly fruitful to refer to the American decisions, particularly when the Supreme Court has more than once clearly enunciated the scope and effect of Article 19 (1) (a) and 19 (2). The test of reasonableness of the restriction has to be considered in each case, in the light of the nature of the right infringed, the purpose of the infringement, the extent and nature of the mischief required to be suppressed and the prevailing social and pattern of reasonableness. Our constitution provides reasonably precise, general guidance in this matter. It would thus be misleading to construe it in the light of American decisions."

---

87 1988 (2) Crimes 173 Kerala
88 Matthan Rahul, *The Law Relating to Computers and the Internet*, Butterworths (India) New Delhi, 1ed. P. 78
89 (1973) 1 SCC 659.
10.2.6 Judicial approach with respect to online gambling

Today online gambling is the phenomenon which generally carried out by various agencies. It is profitable business, however, whether legitimate or illegitimate is depends upon the law of the land. In most of the nations it is lawfully permissible in other, it is illegal. So far in India is concerned, the registered and licence company can carry out the business of online gambling. Most of the states are having their own lottery and gambling business.

Therefore, the problems arise when some of the state permit the online gambling and other are not. When suppose in country 'A', the online gambling is allowed, but the network used in 'A' country is having its base server situated in 'B' country where gambling is illegal. Or the citizens of country 'B' are playing via net the online gambling. Under this situation, country can take lawful action against the agency registered in country 'A', either as it is having server in country 'B' though business is going on in country 'A'.

The issues involved in online gambling and the judicial response can be discussed with following cases.

In State of New York v. World Interactive Gaming Corp90 court granted injunction barring Antigua-based online gaming company from doing business with New York residents. The court held that regardless of whether gambling is legal where the company is based, "The act of entering the bet and transmitting the information from New York via the Internet is adequate to constitute gambling activity within New York State".

The company required users to enter a physical address, and rejected customers whose address was in a state where gambling was illegal. However, the New York attorney general used Nevada address from New York and was able to gain access. The court held this attempt to screen users was not sufficient to shield the site from liability.91

The rational in this case is that the agency which is in the business of online gambling should ensure that to access the website of the agency for playing online gambling should be limited to the territory where online gambling is permissible.

Screen user only’, where person can see the online gambling in the territory where online gambling is prohibited but can not play is not defense under the law.

The another case on this area Reference Re Earth Future Lottery the Prince Edward Island Supreme Court ruled that a charitable lottery was illegal under the Canadian criminal code.

Earth Future Lottery had been granted a license to operate an Internet lottery from its headquarters on Prince Edward Island. The Canadian Criminal Code generally prohibits lotteries, but allows charitable lotteries conducted within their own provinces. The court ruled that although the Internet lottery would operate from Prince Edward Island, it would also reach other provinces and thus it violated the Canadian Criminal Code.

The rational develop in this case have far reaching effect on the area of online gambling.

In United States v. Cohen the Court of Appeals affirmed a decision by a lower court convicting Jay Cohen of operating an illegal offshore Internet sports gambling operation. Cohen operated a bookmaking organization located in Antigua. Customers were required to maintain accounts with the business, and would contact the organization by telephone or Internet to request particular bets. The organization would issue an acceptance and confirmation of each bet.

The Court of Appeals held that the safe harbour provision which shield an individual from criminal liability under certain circumstances, did not apply. The court noted that betting is illegal in New York, and that Cohen’s customers were placing bets by requesting the bets and having them accepted.

In addition, the court found that Cohen had the requisite mens rea, as it was not necessary that he intended to violate the statute so long as he knowingly committed the criminal acts.
Thus the plea of 'safe harbour provision' has been ruled out in this case by the court. Thus mens rea is also an important ingredient to impose criminal liability in the criminal committing online gambling.

10.2.7 Judicial approach on some miscellaneous issue

Lastly, the various other miscellaneous incidences are discussed here which reflect the approach of the judiciary on various issues relating to criminality in cyber space.

In Register.com, Inc. v. Verio, Inc97 court issued a preliminary injunction enjoining Verio, Inc. from either utilizing a search robot to obtain information from Register.com's who is database, or utilizing information derived from that database for mass unsolicited advertising by telephone, direct mail or electronic mail.

Court held that Verio's actions would likely constitute a breach of plaintiff's 'Terms of Use', as well as a violation of both the Computer Fraud and Abuse Act and the Lanham Act and a trespass to chattels. In reaching this conclusion, the court held that Register.com's 'Terms of Use' are likely to create a contract between Register.com and the users of its who is database, notwithstanding the fact that these users are not required to click an "I Agree" button indicating their agreement to be so bound.98

Here the use of database by Verio is sufficient to create link and implied contract come into existence. Thus though it is not necessary that Register.com has neither provided compulsory screen of "I Agree" to its subscribed nor user to impose its 'Terms of Use', the person using its database impliedly having liability not to misuse the database derived from Register.com.

This is very important ratio. Because in India also, there are growing incidences of using web page information and most of the time the files are saved without establishing any 'Term of Use' with the website owner. Therefore, if afterwards the fraud would have been unearthed, the implied condition can be imposed on the user.

97. 126 F. Supp. 2d 238 (S.D.N.Y., December 12, 2000) [USA]
In *United States v. Gilboe*\textsuperscript{99} the Court convicted a person for transportation of money obtained by fraud. Defense based on contention that electronic transfer was not "transportation" was rejected.\textsuperscript{100}

In this case the while interpretation, the golden rule applied by the court. The word 'transportation' include the 'transfer'.

Similarly, *People v. Alan Munn*\textsuperscript{101} the defendant in a harassment case, who asked the readers of a posting on an Internet news group to kill a police officer with family, moved to dismiss on the grounds that New York statute did not cover the Internet. Statute covered communications "by telephone, or telegraph, mail or any other form or written communication".

The Judge held that posting was covered because it was initiated by means of a telephonic communication with the network community.\textsuperscript{102}

Again *State of Utah v. Amoroso*\textsuperscript{103} the state of Utah may criminally prosecute an Illinois corporation for liquor sales to Utah residents over the Internet, through the use of a telephone "800" number, and by mail. Although the Utah appellate court held that it was improper to apply the civil "minimum contacts" analysis, the court held that there was criminal personal jurisdiction in Utah over the defendants based upon the theory that the conduct committed in Illinois caused an unlawful result in Utah.

The court also held that the prosecution was valid under the Twenty-First Amendment and did not violate the Commerce Clause.\textsuperscript{104}

In *United States v. Baker*\textsuperscript{105} & *U.S. v. Alkahabaz*\textsuperscript{106} in this case, a college student who wrote a sado-masochistic fantasy story about one of his classmates and transmitted it to an Internet correspondent could not be prosecuted for interstate transmission of threats to injure or kidnap as there was no showing that the thoughts expressed in the story were "true threats" on which the student intended to act.

\textsuperscript{99} 684 F.2d 235 (2d Cir. 1982) [USA]
\textsuperscript{100} http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16
\textsuperscript{101} Crim. Court Queens Cty., No. 98Q-052574 [USA]
\textsuperscript{102} http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16
\textsuperscript{103} J64 Utah Adv. Rep. 3 (Utah Ct. App. 1999) [USA]
\textsuperscript{104} http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16
\textsuperscript{105} (890 F. Supp. 1375 (E.D. Mich. 1995) [USA])
\textsuperscript{106} (104 F.3d 1492 (6th Cir. Mich. 1997) [USA])
On January 29, 1997, on appeal in *U.S. v. Alkhazaj*, dismissal was affirmed. The Court held that the elements of the charge of threat were not met by email transmitted between two Internet users containing sado-masochistic fantasies about a student known to one of the correspondents.107

In the yes another case, *State of Pennsylvania v. Murgalis*108 the Pennsylvania Superior Court held that the Internet falls under the definition of a "computer system" and the use of e-mail is "accessing a computer" under a Pennsylvania criminal statute.

The defendant was convicted of unlawful use of a computer, arising from his failure to deliver items purchased on-line by customers, and his passing on bad cheques to suppliers. The Pennsylvania statute prohibits the use of a computer system with the intent to defraud. The court rejected the defendant’s argument that the Internet is not a "computer system".109

*United States v. Sills*110 a police officer was charged with using software and a radio scanner to intercept alphanumeric pager messages in violation of the Electronic Communications Privacy Act.

The judge denied the officer's motion to dismiss, holding that the interception did not fall within the Act's exemption for telex-only pagers, and rejecting a claim of selective prosecution.111

*Firth v. State of New York*112 the plaintiff claimed that publication of an alleged libel on the Internet was "continuous publication", which would extend the statute of limitations.

The court held that the statute would run from the date the material was first posted, rather than continuously. On October 29, 2001, the New York Appellate Division Court affirmed the decision.113

*United States v. Gray*114 the court held that child pornography discovered during a search conducted pursuant to obtaining a warrant for materials related to computer tampering was admissible. Defendant argued that files with the .JPG extension were presumptively pictures and not related to subject of search. Court noted

---

108 No. 189 MDA 1999 (Pu. Super. Ct., June 2, 2000) [USA]
110 S.D.N.Y., April 2000 [USA]
112 N.Y. Court of Claims, March 2000 [USA]
114 78 F. Supp.2d 524 (E.D. Va. 1999) [USA]
that hackers frequently mislabel files, and FBI agents were not required to take file names at face value.\textsuperscript{115}

*Doherty v. Registry of Motor Vehicles*\textsuperscript{116} the court held that an electronically-transmitted police report satisfied the requirement of a signed writing under the state's perjury law.\textsuperscript{117}

*In re Doubleclick Inc. Privacy Litigation*\textsuperscript{118}: the Court dismissed the claims advanced by the plaintiff under the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the Wiretap Act arising out of Doubleclick's use and placement of "cookies" on plaintiffs' computers.

Doubleclick uses such "cookies" to gather information about the users' use of Doubleclick client web sites. Since Doubleclick's clients consented to such information being gathered, the court held that Doubleclick's activities did not run afoul of either the Electronic Communications Privacy Act or the Wiretap Act.

The court also dismissed the claims, which the plaintiffs advanced under the Computer Fraud and Abuse Act because any damages caused by Doubleclick's activities did not meet the threshold required by the Computer Fraud and Abuse Act. Finally, the court, having dismissed all of the plaintiffs' federal claims, declined to retain jurisdiction over plaintiffs' state law claims, and dismissed the action.\textsuperscript{119}

*United States of America V. Robert Tappan Morris*\textsuperscript{120} in 1988, Morris was a first-year graduate student in Cornell University's computer science Ph.D. program. Through undergraduate work at Harvard and in various jobs he had acquired significant computer experience and expertise.

When Morris entered Cornell, he was given an account on the computer at the Computer Science Division. This account gave him explicit authorization to use computers at Cornell. Morris engaged in various discussions with fellow graduate students about the security of computer networks and his ability to penetrate it.

\textsuperscript{115} http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16
\textsuperscript{116} 97CV0050 (Mass. Dist. Ct., Suffolk Cty. Charlestown Div., May 28, 1997) [USA]
\textsuperscript{117} http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16
\textsuperscript{118} 00 Civ. 0641 (S.D.N.Y., March 28, 2001) [USA]
\textsuperscript{119} http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16
\textsuperscript{120} 928 F.2d 504; 1991 U.S. App. LEXIS 3682 United States Court Of Appeals For The Second Circuit[USA]
On January 29, 1997, on appeal in *U.S. v. Alkhazae*, dismissal was affirmed. The Court held that the elements of the charge of threat were not met by email transmitted between two Internet users containing sado-masochistic fantasies about a student known to one of the correspondents.\textsuperscript{107}

In the yes another case, *State of Pennsylvania v. Murgalis*\textsuperscript{108} the Pennsylvania Superior Court held that the Internet falls under the definition of a "computer system" and the use of e-mail is "accessing a computer" under a Pennsylvania criminal statute.

The defendant was convicted of unlawful use of a computer, arising from his failure to deliver items purchased on-line by customers, and his passing of bad cheques to suppliers. The Pennsylvania statute prohibits the use of a computer system with the intent to defraud. The court rejected the defendant's argument that the Internet is not a "computer system".\textsuperscript{109}

*United States v. Silk*\textsuperscript{110} a police officer was charged with using software and a radio scanner to intercept alphanumeric pager messages in violation of the Electronic Communications Privacy Act.

The judge denied the officer's motion to dismiss, holding that the interception did not fall within the Act's exemption for te-sole only pagers, and rejecting a claim of selective prosecution.\textsuperscript{111}

*First v. State of New York*\textsuperscript{112} the plaintiff claimed that publication of an alleged libel on the Internet was "continuous publication", which would extend the statute of limitations.

The court held that the statute would run from the date the material was first posted, rather than continuously. On October 29, 2001, the New York Appellate Division Court affirmed the decision.\textsuperscript{113}

*United States v. Gray*\textsuperscript{114} the court held that child pornography discovered during a search conducted pursuant to obtaining a warrant for materials related to computer tampering was admissible. Defendant argued that files with the .JPG extension were presumptively pictures and not related to subject of search. Court noted

\textsuperscript{107} http://www.asianlaw.org/cyberlaw/library/ec/ec_caselaw.htm Accessed on 05 June 2004, 23:35:16
\textsuperscript{108} No. 189 MDA 1999 (Pa, Super. Ct., June 2, 2000) [USA]
\textsuperscript{109} http://www.asianlaw.org/cyberlaw/library/ec/ec_caselaw.htm Accessed on 05 June 2004, 23:35:16
\textsuperscript{110} S.D.N.Y., April 2000 [USA]
\textsuperscript{111} http://www.asianlaw.org/cyberlaw/library/ec/ec_caselaw.htm Accessed on 05 June 2004, 23:35:16
\textsuperscript{112} N.Y. Court of Claims, March 2000 [USA]
\textsuperscript{113} http://www.asianlaw.org/cyberlaw/library/ec/ec_caselaw.htm Accessed on 05 June 2004, 23:35:16
\textsuperscript{114} 78 F. Supp.2d 524 (E.D. Va. 1999) [USA]
that hackers frequently mislabel files, and FBI agents were not required to take file names at face value.\footnote{115}

_Doherty v. Registry of Motor Vehicles\footnote{116} the court held that an electronically-transmitted police report satisfied the requirement of a signed writing under the state's perjury law.\footnote{117}

_In re Doubleclick Inc. Privacy Litigation\footnote{118} the Court dismissed the claims advanced by the plaintiff under the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the Wiretap Act arising out of Doubleclick's use and placement of "cookies" on plaintiffs' computers.

Doubleclick uses such "cookies" to gather information about the users' use of Doubleclick client web sites. Since Doubleclick's clients consented to such information being gathered, the court held that Doubleclick's activities did not run afoul of either the Electronic Communications Privacy Act or the Wiretap Act.

The court also dismissed the claims, which the plaintiffs advanced under the Computer Fraud and Abuse Act because any damages caused by Doubleclick's activities did not meet the threshold required by the Computer Fraud and Abuse Act. Finally, the court, having dismissed all of the plaintiffs' federal claims, declined to retain jurisdiction over plaintiffs' state law claims, and dismissed the action.\footnote{119}

_United States of America V. Robert Tappan Morris\footnote{120} in 1988, Morris was a first-year graduate student in Cornell University's computer science Ph.D. program. Through undergraduate work at Harvard and in various jobs he had acquired significant computer experience and expertise.

When Morris entered Cornell, he was given an account on the computer at the Computer Science Division. This account gave him explicit authorization to use computers at Cornell. Morris engaged in various discussions with fellow graduate students about the security of computer networks and his ability to penetrate it.

\footnotetext{115}{http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16}
\footnotetext{116}{97CV0050 (Mass. Dist. Ct., Suffolk Cty. Charlestown Div., May 28, 1997) [USA]}
\footnotetext{117}{http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16}
\footnotetext{118}{00 Civ. 0641 (S.D.N.Y., March 28, 2001) [USA]}
\footnotetext{119}{http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm Accessed on 05 June 2004, 23:35:16}
\footnotetext{120}{928 F.2d 504; 1991 U.S. App. LEXIS 3682 United States Court Of Appeals For The Second Circuit[USA]}

In October 1988, Morris began work on a computer program, later known as the Internet "worm" or "virus". The goal of this program was to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered.

The tactic he selected was the release of a worm into network computers. Morris designed the program to spread across a national network of computers after being inserted at one computer location connected to the network. Morris released the worm into the Internet.

Morris sought to program the INTERNET worm to spread widely without drawing attention to itself. The worm was supposed to occupy little computer operation time, and thus not interfere with normal use of the computers. Morris programmed the worm to make it difficult to detect and read, so that other programmers would not be able to "kill" the worm easily.

Morris also wanted to ensure that the worm did not copy itself onto a computer that already had a copy. Multiple copies of the worm on a computer would make the worm easier to detect and would bog down the system and ultimately cause the computer to crash. Therefore, Morris designed the worm to "ask" each computer whether it already had a copy of the worm. If it responded "no," then the worm would copy onto the computer; if it responded "yes," the worm would not duplicate. However, Morris was concerned that other programmers could kill the worm by programming their own computers to falsely respond "yes" to the question. To circumvent this protection, Morris programmed the worm to duplicate itself every seventh time it received a "yes" response.

As it turned out, Morris underestimated the number of times a computer would be asked the question, and his one-out-of-seven ratio resulted in far more copying than he had anticipated. The worm was also designed so that it would be killed when a computer was shut down, an event that typically occurs once every week or two. This would have prevented the worm from accumulating on one computer, had Morris correctly estimated the likely rate of re-infection.

Morris identified four ways in which the worm could break into computers on the network:
i. through a "hole" or "bug" (an error) in SEND MAIL, a computer program that transfers and receives electronic mail on a computer;

ii. through a bug in the "finger demon" program, a program that permits a person to obtain limited information about the users of another computer;

iii. through the "trusted hosts" feature, which permits a user with certain privileges on one computer to have equivalent privileges on another computer without using a password; and

iv. through a program of password guessing, whereby various combinations of letters are tried out in rapid sequence in the hope that one will be an authorized user's password, which is entered to permit whatever level of activity that user is authorized to perform.

On November 2, 1988, Morris released the worm from a computer at the Massachusetts Institute of Technology. MIT was selected to disguise the fact that the worm came from Morris at Cornell. Morris soon discovered that the worm was replicating and re-infesting machines at a much faster rate than he had anticipated.

Ultimately, many machines at locations around USA either crashed or became "catatonic". When Morris realized what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent re-infection. However, because the network route was clogged, this message did not get through until it was too late.

Computers were affected at numerous installations, including leading universities, military sites, and medical research facilities. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000.

Morris was found guilty, following a jury trial, of violating 18 U.S.C. @ 1030(a)(5)(A). He was sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision.
The major issue raised in this case was what satisfies the statutory requirement of "access without authorization".

Subsection 1030(a)(5)(A) penalizes the conduct of an individual who "intentionally accesses a Federal interest computer without authorization". The accused contended that his conduct constituted, at most, "exceeding authorized access" rather than the "unauthorized access" that the subsection punishes.

The Court held that under the traditional standard Morris was authorized to use computers at Cornell, Harvard, and Berkeley, all of which were on INTERNET. As a result, Morris was authorized to communicate with other computers on the network to send electronic mail (SEND MAIL), and to find out certain information about the users of other computers (finger demon). The question is whether Morris's transmission of his worm constituted exceeding authorized access or accessing without authorization.

The Court held that Morris's conduct fell well within the area of unauthorized access.

"Morris did not use either of those features in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers".

The Court also held that although initial insertion of the worm simply exceeded the accused's authorized access, the evidence demonstrated that the worm was designed to spread to other computers at which he had no account and no authority, express or implied, to unleash the worm program.

Moreover, there was also evidence that the worm was designed to gain access to computers at which he had no account by guessing their passwords. The Court held that the evidence supported the conclusion that the accused accessed without authority as opposed to merely exceeding the scope of his authority.121

10.2.8 Judicial response with respect to 'Theft of information'

In the modern world, information is life blood of all transactions. The Computer Technology use to be utilized for the purpose of dissemination of

information from its source to destination. Therefore, protection and security of
information in Cyberspace is a prime issue. However, it has been observed that most of
the time, there is information theft occurs. This phenomenon is more dangerous in case
of the theft committed from the computers of military or para-military institution or
even from government offices. It may cause to leak the important information in the
hands of those which would misuse it. Therefore, utmost care should be taken for the
protection of important information. Even the NASA websites was hacked by the
hackers and there have been incidences of information theft from most important
computers of the world! The hackers, it seems, not deter as they are having special
facility to execute their theft even without remaining present within the premises or
jurisdiction. Only requirement for them in Cyberspace is that the computer must be
connected in the networking. Most of the time, the thieves use fake identity for
committing theft and use known identity to dodge the computers.

The famous case in America on the theft of information is the United States v
PHILIP CUMMINGS'. In the present case the United States Attorney and the Assistant
Director in Charge of the New York Field Office of the FBI, arrested the defendant,
PHILIP CUMMINGS, in what authorities believe to be the largest identity theft case in
U.S. history.

The United States charged PHILIP CUMMINGS with wire fraud and
conspiracy in connection with his participation in a massive identity theft scheme that
spanned nearly three years and involved more than 30,000 victims. As alleged in the
Complaint, CUMMINGS worked at Teledata Communications Inc. ("TCI"), a company
in Long Island that provided the computerized means for banks and other entities to
obtain consumer credit information from the three commercial credit history bureaus
- Equifax, Experian and TransUnion. TCI provided software and other computerized
devices to its client companies that enabled these companies, through the use of
confidential computer passwords and subscriber codes, to access and download credit
reports of consumers for legitimate business purposes. CUMMINGS worked at TCI
from about mid-1999 through about March 2000 as a Help-Desk employee, and was
responsible for helping TCI's clients. As such, he had access to these companies'
confidential passwords and codes. With these codes, he had the ability to access and
download credit reports himself, it was charged.

Starting in early 2000, CUMMINGS agreed to provide credit reports to a co-
conspirator who cooperated witness in the investigation ("CW"), in return for money.
CW knew individuals who were willing to pay up to $60 per credit report, and CW offered to split that money with CUMMINGS, it was charged. Thereafter, CW dealt with 20 or more individuals in the Bronx and Brooklyn, who would bring lists to CW filled with names and addresses and/or Social Security numbers, and would ask CW to provide credit reports in those people's names. They would then pay him $60 for each credit report that he was able to provide to them, it was charged, and CW, in turn, would split that money with CUMMINGS. CW began receiving lists from these co-conspirators in the beginning, he would contact CUMMINGS, and CUMMINGS would bring a laptop computer to the CW's home in New York and download the credit reports and give them to CW. CW in turn would sell them to his co-conspirators on the street. CUMMINGS provided passwords and codes to CW that enabled CW to access all three Credit Bureaus - Equifax, Trans-Union and Experian - over time. At various points in the scheme, when CW found that a code and password that CW had been using no longer worked, he allegedly called CUMMINGS. CUMMINGS would then allegedly give him a new password and code to use to continue the scheme.

This happened on numerous occasions. The other co-conspirators to whom CW sold the credit reports provided, in the aggregate, tens of thousands of names and hundreds of thousands of dollars to CW for consumer credit reports. CW provided the credit reports to these other co-conspirators and split the money that they provided to CW with CUMMINGS.

One entity whose confidential TCI password and subscriber code were allegedly misappropriated in the scheme was Ford Motor Credit Corp. at its Grand Rapids, Michigan, branch. That branch's password and code were used for approximately 10 months to download approximately 15,000 credit reports from Experian. Ford discovered the scheme after reviewing bills sent by Experian for those credit histories and receiving numerous complaints from consumers who had been the subject of identity theft and fraud. After searching its databases, Experian found that the passwords and subscriber codes of Washington Mutual Bank in Florida and Washington Mutual Finance Company in Crossville, Tennessee, had also been compromised, resulting in approximately 6,000 more credit reports for consumers being improperly downloaded.

According to the Complaint, Equifax determined that the password and subscriber codes for Ford's Decatur, Illinois, branch had been used improperly to download 1,300 credit reports from its databases in September and October 2002. The
passwords and codes of Washington Mutual Finance's branch in St. Augustine, Florida, were used to download another 1,100 credit reports, and more than 4,000 additional credit reports were downloaded using the passwords and codes of six more entities: Dollar Bank in Cleveland, Ohio; Sarah Bush Lincoln Health Center in Illinois; the Personal Finance Company in Frankfort, Indiana; the Medical Bureau in Clearwater, Florida; Vintage Apartments in Houston, Texas; and Community Bank of Chaska in Chaska, Minnesota.

Central Texas Energy Supply's codes were used improperly to download approximately 4,500 credit reports from TransUnion in September 2002. The number of victims in this case exceeds 30,000, and the Government is in the process of determining the extent of the loss. To date, more than $2.7 million in financial loss has been confirmed. Consumers whose credit reports have been stolen in this scheme have reported many forms of identity fraud. As alleged in the Complaint, bank accounts holding tens of thousands of dollars in savings have been depleted; credit cards have been used to the tune of thousands of dollars without authorization; address changes have been made to accounts at various financial institutions; checks, debit cards, ATM cards and credit cards have been sent to unauthorized locations; and identities of victims have been assumed by others.

In a related case, LINUS BAPTISTE was arrested on October 29, 2002 on a wire fraud charge related to the CUMMINGS case. According to that Complaint, phone numbers registered to BAPTISTE's residence were used to dial into Equifax's databases and download 400 - 600 credit reports in August 2002 in the scheme. Credit reports, laptop computers and a document bearing CUMMINGS' name were found in BAPTISTE's home.

In a related case involving fraud perpetrated on several of these victims, on July 30, 2002, a defendant using the name HAKEEM MOHAMMED was charged with mail fraud in connection with an address change made to a line of credit opened by two of the Ford victims and the opening of accounts and lines of credit in the names of two other Ford victims. MOHAMMED entered a guilty plea to mail fraud and conspiracy charges on October 2, 2002, and is sentenced before United States District Judge GERALD E. LYNCH on January 8, 2003.

CUMMINGS is presented in Manhattan federal court this afternoon on the Complaint unsealed today. If convicted, CUMMINGS faces, with respect to the wire
fraud charge, a maximum term of 30 years' imprisonment and a maximum fine of $1 million or twice the pecuniary gain or loss resulting from the offense. CUMMINGS faces, with respect to the conspiracy charge, a maximum term of 5 years' imprisonment and a maximum fine of $250,000, or twice the gross gain or loss resulting from the crime.

With a few keystrokes, these men essentially picked the pockets of tens of thousands of Americans and, in the process, took their identities, stole their money and swiped their security. These charges and the potential penalties underscore the severity of the crimes. We will pursue and prosecute with equal vigor others who may be involved. The defendants took advantage of an insider's access to sensitive information in much the same way that a gang of thieves might get the combination to the bank vault from an insider. But the potential windfall was probably far greater than the contents of a bank vault and, using 21st century technology, they didn't even need a getaway car. Using the same technology, we determined what was done and who did it, proving that technology is a double-edged sword.122

10.2.9 The Judicial approach towards 'E-mail bombing'

Though e-mail bombing is not too frequent in India, but still there is quite threat from it. The basis for doing such act and using technology for harassment to the person with whom this e-mail bomber wants to take revenge. Thus, this is common phenomenon where person want to settle his score by using computer technology by remaining hidden behinds the terminals. Though superficially, it seems quite easy, it has great potential to sustain loss of corers of rupees. Particularly, in trade business, it may irritated the customers, may cause wrong communication and spoil the commercial relations. Therefore, it is utmost necessary to discuss such issues at length.

The famous incidence occurs in India. Solving their first case, the officers of the Cyber Crime Police Station have arrested K.R. Vijaya Kumar, an electronics engineer with the Bangalore office of Phoenix Global Solutions (India) Limited, for allegedly downing the company's e-mail server in the U.S.

The Cyber Crime Police Station of the CoD, the first of its kind in the country, registered a case on November 12 following a complaint by the company. The

complaint said that a hacker had sent e-mails to the firm's head office in the U.S., threatening it to close down its India operations or face the consequence.

After the U.S. office ignored them, Kumar sent a similar mail. Later, he downed the e-mail server, and sent a mail boasting of his "enormous power and reach".

Subsequently, the firm lodged the complaint. The Deputy Superintendent of Police, Mr. K.Srikanta, took up the investigation. Kumar was arrested under the Information Technology Act, 2000. He was produced before the 1st Additional City Metropolitan Magistrate Court, Bangalore, which remanded him in judicial custody.123

The case is pending before the court.

The next incidence is also eye opening.

Former employees of Mphasis have been arrested for robbing $350,000 from Citibank accounts based in the USA. The latest scam has caused a stir in the booming outsourcing business. The police said that the investigations into the Rs 1.5 crore cyber crimes have revealed a fake ration card from the prime accused, Ivan Samuel Thomas.

The former Mphasis staff dealing with Citibank's customers tricked four of them into giving out the PIN numbers to their accounts, allowing the staff to transfer funds into the bank accounts of other 'gang' members.

Sanjay Jadhav, ACP, has told the court Thomas's e-mail password had been changed after his arrest on April 6, leading them to suspect others were involved as well.

The police said that Stephen Daniel, one of the accused was a Defense Research and Development Organization employee and they were probing his possible involvement in other cases. The police also revealed that an additional $75,000 was also withdrawn from the US citizens' Citibank accounts. Public prosecutor D.T. Sonar told the court that the police had been able to recover Rs 13 lakh from the accused.

The Judicial Magistrate has heard the case and extended the police custody of Ivan Thomas, Ginny Thomas George, Nitin Madhav Valkar, Vijay More, Saundraj Ramanujam and Satish Madhukar Parab.124

Another famous case on the 'Email bombing' is *El Segundo v Bret McDanel*. In the present case a federal judge in Los Angeles today convicted a former Southern California man of maliciously bombarding the computer system of an El Segundo computer messaging company with thousands of email messages.

Bret McDanel, who used the moniker “Secret Squirrel,” is a 29-year-old resident of Fiddletown, California, was found guilty of maliciously sending thousands of email messages to a computer server operated by Tornado Development, Inc. in September 2000. By finding McDanel guilty, United States District Judge Lourdes G. Baird found that the defendant acted with the intent to cause damage to Tornado’s mail server.

The evidence presented at trial showed that McDanel, who worked at Tornado from June 1999 until February 2000, committed the crime to retaliate against Tornado. The prosecutors argued to Judge Baird that McDanel harbored resentment against his former employer and that he planned to start a competitor messaging company.

McDanel sent thousands of email messages and overloaded the Tornado computer server. Additionally, the emails he sent contained a link to a web site he had created where he revealed confidential information about Tornado technology that McDanel had learned while employed there.

During the trial, the government also presented evidence that McDanel had attacked the computer system of another former employer in New Jersey in 1997.

This was the first case to go to trial in Los Angeles brought under the “Computer Fraud and Abuse Act,” the federal statute covering computer abuse and malicious spamming.

Judge Baird sentenced McDanel on September 16 for five years in federal prison.125


10.2.10 The judicial pronouncement on 'Data Diddling'

Data diddling is also considered as one of the most dangerous type of crime. However, it is quite often seen that no such words is either define or made punishable by the I.T. Act, 2000. Though this type of crime is not very frequent in India so far, however, in developed countries there is no less number of cases on the topic. The famous case in this respect is Viewsonic Corporation v. Andy Garcia. The facts of the case are follows.

A man previously employed at the Walnut office of the Viewsonic Corporation was arrested federal charges of hacking into the company's computer system and wiping out critical data, acts that shut down a computer server that was central to the company's foreign operations.

Andy Garcia, 39, of Montebello, was arrested pursuant to an indictment returned January 28 by a federal grand jury in Los Angeles. The indictment accuses Garcia of unauthorized access to a protected computer and of being a convicted felon in possession of a firearm.

Viewsonic Corporation is a manufacturer of computer monitors that generates more than $1 billion a year in revenues. Garcia was the network administrator at Viewsonic's Walnut office, where he was in charge of several computer servers and had access to system passwords for management employees.

According to court documents, on April 14, 2002, approximately two weeks after Garcia was terminated, Garcia allegedly accessed Viewsonic's computer system and deleted critical files on one of the servers that he had maintained while employed by the company. The loss of these files rendered the server inoperative, and Viewsonic's Taiwan office was unable to access important data for several days.

Garcia was also charged with possession of a semi-automatic assault weapon found at his home. His possession of such a weapon is unlawful because he was previously convicted of two felonies.

Garcia is expected to make an initial appearance on the charges in United States District Court in Los Angeles. If convicted, he faces a maximum possible sentence of 15 years in federal prison.126

---

10.2.11 Cases on 'Viruses'

The United States v. David L. Smith case is famous to explain the judicial position with respect to 'virus'. On May 1, 2001, the New Jersey man accused of unleashing the "Melissa" computer virus in 1999, causing millions of dollars in damage and infecting untold numbers of computers and computer networks, was sentenced to 20 months in federal prison.

David L. Smith of Aberdeen Township in Monmouth County, was ordered to serve three years of supervised release after completion of his prison sentence and was fined $5,000. U.S. District Judge Joseph A. Greenaway Jr. further ordered that, upon release, Smith not be involved with computer networks, the Internet or Internet bulletin boards unless authorized by the Court. And Smith must serve 100 hours of community service upon release. The supervised community service would somehow put to use Smith’s technology experience.

Smith pleaded guilty on Dec. 9, 1999, in state and federal court to computer-related crimes. The two prosecutions are the result of cooperative state and federal investigations of Smith, who, at his guilty plea, admitted spreading the computer virus across North America from his home computer in Aberdeen Township. He said that he constructed the virus to evade anti-virus software and to infect computers using the Windows 95, Windows 98 and Windows NT operating systems and the Microsoft Word 97 and Word 2000 word processing programs. The Melissa virus appeared on thousands of email systems on March 26, 1999, disguised as an important message from a colleague or friend. The virus was designed to send an infected email to the first 50 email addresses on the users' mailing lists. Such emails would only be sent if the computers used Microsoft Outlook for email.

Because each infected computer could infect 50 additional computers, which in turn could infect another 50 computers, the virus proliferated rapidly and exponentially, resulting in substantial interruption or impairment of public communications or services. According to reports from business and government following the spread of the virus, its rapid distribution disrupted computer networks by overloading email servers, resulting in the shutdown of networks and significant costs to repair or cleanse computer systems.

Smith described in state and federal court how, using a stolen America Online account and his own account with a local Internet service provider, he posted an
infected document on the Internet newsgroup "Alt.Sex." The posting contained a message enticing readers to download and open the document with the hope of finding passcodes to adult-content websites.

Opening and downloading the message caused the Melissa virus to infect victim computers. The virus altered Microsoft word processing programs such that any document created using the programs would then be infected with the Melissa virus. The virus also lowered macro security settings in the word processing programs. The virus then proliferated via the Microsoft Outlook program, causing computers to send electronic email to the first 50 addresses in the computer user's address book. Smith acknowledged that each new email greeted new users with an enticing message to open and, thus, spread the virus further. The message read: "Here is that document you asked for... don't show anyone else."

On April 1, 1999, members of the New Jersey State Police High Technology Crime Unit, Special Agents of the FBI and investigators from the Monmouth County Prosecutor's Office arrested Smith at his brother's house in Eatontown. The arrest followed a tip from a representative of America Online to the head of the Computer Analysis and Technology Unit in the state Division of Criminal Justice.

Smith pleaded guilty in federal court to one-count Information, charging him with knowingly spreading a computer virus with the intent to cause damage. The charge carries a maximum prison sentence of five years in prison and a $250,000 fine.

On the same day as the federal guilty plea, Smith pleaded guilty in Superior Court in Freehold to a one-count accusation, charging the second-degree offense of computer-related theft. The state has recommended a statutory maximum sentence of 10 years in prison. Smith also faces state fines of up to $150,000.

The state plea agreement provides that the federal sentencing would occur first and that, at the subsequent state sentencing, New Jersey authorities would recommend that the state sentence run co-terminously and concurrently to the federal sentence.127

127 http://www.asianlaws.org/projects/network_crimes.htm Accessed on 05.06.2004 at 22:38:06
10.2.12 Various dimensions of legal problems existing in Cyber space and judicial response

The problem before the judiciary not only arise with special cyber crimes but sometime the problem of having different dimensions may come out which gives rise to some crucial issues relating to implementation of law in cyber space. Some of such issues can be discussed as follows.

1. Computer print-outs can be admitted as documentary evidence

In an unprecedented ruling, a TADA court at Mumbai has held that computer printouts can be admitted as documentary evidence. The ruling was delivered on 6.7.2000 by the Judge Shri Pramod Kode before whom the CBI examined an official of the Mahanagar Telephone Limited (MTNL), to corroborate his charges against film star Sanjay Dutt of having made an international call from his residence to Dubai - based Aneesh Ibrahim, brother of Dawood Ibrahim.

During the examination of the witnesses, computer print-outs containing the called numbers were produced as exhibits. These print-outs were taken from magnetic tapes on which the Bandra Telephone Exchange had recorded outgoing and incoming calls, to places within and outside India in the year 1993. The investigating officer had collected only the print-outs and not the magnetic tapes. The tapes were preserved for a period of three years by MTNL and later destroyed following the usual practice.

The prosecution contended, that the computer print-out was primary evidence within the meaning of section 62 of the Indian Evidence Act, as print-outs were made by a uniform process and, therefore, deserved to be exhibited. These were the result of records contained in the magnetic tape automatically made at the exchanges regarding respective calls made or received. Such print-outs were not copies of the matters recorded on the magnetic tape and could, therefore, be exhibited. The defence argued that the print-outs produced in the court were not original print-outs taken for the purpose of making bills. The primary evidence related to the alleged telephone call was the magnetic tape which had not been produced before the court. The defence also pleaded that the investigating agency had failed to collect the magnetic tape, and therefore, no case was made out under section 63 to permit secondary evidence. Hence, the document cannot be marked as exhibit.
The court observed that the print-outs are not a copy of the magnetic tape because the tape by itself cannot be termed as a document. It does not fall within the definition of a document under section 3 of Indian Evidence Act. Evidence is something which can be perceived by the human senses. Matter, which cannot be perceived by the human senses by a Judge cannot fall within the definition of the word 'document' or the word 'evidence'. Even if the magnetic tape had been produced before the court, the court would have been unable to directly perceive i.e. to read, hear or see the matter stored on it and consequently, would have been unable to act upon the said matter. The print-outs, on the other hand constitute the direct evidence of the matter. They were taken by technicians from the computer in the presence of the witness and after satisfying that at the relevant time the computer was properly working. It was therefore, ruled that the print-outs were primary evidence.  

2. Combined Civil and Criminal cases maintainable

The Supreme Court recently held that a complaint alleging both civil wrong and a criminal offence is maintainable in a court of law. The Court observed

"It is settled law that facts may give rise to a civil claim and also amount to an offence. Merely because a civil claim is maintainable it does not mean that the criminal complaint cannot be maintained."

The Court's observations followed an appeal by Lalmuni Devi against a Patna High Court order quashing her complaint. The High Court held that since the complaint disclosed a civil wrong, initiating criminal prosecution would be an abuse of the legal process. The appellant's complaint alleged that some persons had fraudulently got her father to execute a gift deed. After an inquiry, the Magistrate dismissed the complaint. On appeal, the Sessions Court, however, remanded the matter back to the Magistrate. Taking cognizance of the complaint, the Magistrate then summoned the accused named in the complaint. Aggrieved by the order, the accused challenged the Magistrate's order in the High Court that quashed the complaint.  

Thus with reference to the case and read it with the IT Act, 2000, which provided two different types of remedies i.e. civil and criminal nature, the both cases can be combined.

128 http://www.w3.org/TR/REC-html40/ Accessed on 31.03.2005 at 02:52:09
10.3 Conclusion

Thus theses are the various ways by which judiciary shape the various disputes in the Cyberspace. The courts at national as well as international level have dealt according to their own law of the land to the problems arising in the Cyberspace. In India, the development is less marked. The prosecution of crimes relating to obscenity, pornography, online gambling, e-mail threats, defamation etc., etc., do not appear to have generated any considerable body of jurisprudential development. The tests used by Indian courts to identifying these issues seemed to be very important in Cyberspace are comparatively less detailed, when held up against the test used in the other developed nation. This may be because of the fact, that since the computer technology is having basically western origin and these nations 'trigger on' their judicial responses very early in the Cyberspace.

However, this is the very high time. Today, to discuss the concept like 'Global village' seems to be childish because everybody in any corner of the world is only at hand distance from other. Just pick up your mobile from pocket and dial numbers! Thus when the barriers of time, place, and distance is disappearing in the Cyberspace, how so far the national boundaries may demarcate the difference? Therefore, today all nations across the world should have to come forward with their respective tools of controlling Cyber crime. It is a time when we can say, 'better late than never'.