CYBER LAW & INFORMATION TECHNOLOGY

*by **Talwant Singh** Addl. Distt. & Sessions Judge, Delhi*

Success in any field of human activity leads to crime that needs mechanisms to control it. Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. The law is as stringent as its enforcement. Crime is no longer limited to space, time or a group of people. Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies. Back in 1990, less than 100,000 people were able to log on to the Internet worldwide. Now around 500 million people are hooked up to surf the net around the globe.

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

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

IT professionals need good definitions of cybercrime in order to know when (and what) to report to police, but law enforcement agencies *must* have statutory definitions of specific crimes in order to charge a criminal with an offense. The first step in specifically defining individual cybercrimes is to sort all the acts that can be considered cybercrimes into organized categories.

United Nations' Definition of Cybercrime

Cybercrime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of the crime. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

a. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Of course, these definitions are complicated by the fact that an act may be illegal in one nation but not in another.

There are more concrete examples, including

i. Unauthorized access

ii Damage to computer data or programs

iii Computer sabotage

iv Unauthorized interception of communications

v Computer espionage

These definitions, although not completely definitive, do give us a good starting point—one that has some international recognition and agreement—for determining just what we mean by the term ***cybercrime.***

In Indian law, cyber crime has to be voluntary and willful, an act or omission that adversely affects a person or property. The IT Act provides the backbone for e-commerce and India's approach has been to look at e-governance and e-commerce primarily from the promotional aspects looking at the vast opportunities and the need to sensitize the population to the

possibilities of the information age. There is the need to take in to consideration the security aspects.

In the present global situation where cyber control mechanisms are important we need to push cyber laws. Cyber Crimes are a new class of crimes to India rapidly expanding due to extensive use of internet. Getting the right lead and making the right interpretation are very important in solving a cyber crime. The 7 stage continuum of a criminal case starts from **perpetration** to **registration** to **reporting**, **investigation**, **prosecution**, **adjudication** and **execution**. The system can not be stronger than the weakest link in the chain. In India, there are 30 million policemen to train apart from 12,000 strong Judiciary. Police in India are trying to become cyber crime savvy and hiring people who are trained in the area. Each police station in Delhi will have a computer soon which will be connected to the Head Quarter.. The pace of the investigations however can be faster; judicial sensitivity and knowledge need to improve. Focus needs to be on educating the police and district judiciary. IT Institutions can also play a role in this area.

Technology nuances are important in a spam infested environment where privacy can be compromised and individuals can be subjected to become a victim unsuspectingly. We need to sensitize our investigators and judges to the nuances of the system. Most cyber criminals have a counter part in the real world. If loss of property or persons is caused the criminal is punishable under the IPC also. Since the law enforcement agencies find it is easier to handle it under the IPC, IT Act cases are not getting reported and when reported are not necessarily dealt with under the IT Act. A lengthy and intensive process of learning is required.

A whole series of initiatives of cyber forensics were undertaken and cyber law procedures resulted out of it. This is an area where learning takes place every day as we are all beginners in this area. We are looking for solutions faster than the problems can get invented. We need to move faster than the criminals.

The real issue is how to prevent cyber crime. For this, there is need to raise the probability of apprehension and conviction. India has a law on evidence that considers admissibility, authenticity, accuracy, and completeness to convince the judiciary. The challenge in cyber crime cases includes getting evidence that will stand scrutiny in a foreign court.

For this India needs total international cooperation with specialised agencies of different countries. Police has to ensure that they have seized exactly what was there at the scene of crime, is the same that has been analysed and the report presented in court is based on this evidence. It has to maintain the chain of custody. The threat is not from the intelligence of criminals but from our ignorance and the will to fight it. The law is stricter now on producing evidence especially where electronic documents are concerned.

The computer is the target and the tool for the perpetration of crime. It is used for the communication of the criminal activity such as the injection of a virus/worm which can crash entire networks.

The Information Technology (IT) Act, 2000, specifies the acts which have been made punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T., certain omissions and commissions of criminals while using computers have not been included. With the legal recognition of Electronic Records and the amendments made in the several sections of the IPC vide the IT Act, 2000, several offences having bearing on cyber-arena are also registered under the appropriate sections of the IPC.

During the year 2003, 60 cases were registered under IT Act as compared to 70 cases during the previous year thereby reporting a decline of 14.3 percent in 2003 over 2002. Of the total 60 cases registered under IT Act 2000, around 33 percent (20 cases) relate to Obscene Publication / Transmission in electronic form, normally known as cases of cyber pornography. 17 persons were arrested for committing such offences during 2003.

There were 21 cases of Hacking of computer systems wherein 18 persons were arrested in 2003. Of the total (21) Hacking cases, the cases relating to Loss/Damage of computer resource/utility under Sec 66(1) of the IT Act were to the tune of 62 percent (13 cases) and that related to Hacking under Section 66(2) of IT Act were 38 percent (8cases).

During 2003, a total of 411 cases were registered under IPC Sections as compared to 738 such cases during 2002 thereby reporting a significant decline of 44 percent in 2003 over 2002. Andhra Pradesh reported more than half of such cases (218 out of 411) (53 percent).

Of the 411 cases registered under IPC, majority of the crimes fall under 3 categories viz. Criminal Breach of Trust or Fraud (269), Forgery (89) and Counterfeiting (53).

Though, these offences fall under the traditional IPC crimes, the cases had the cyber tones wherein computer, Internet or its related aspects were present in the crime and hence they were categorised as Cyber Crimes under IPC.

During 2003, number of cases under Cyber Crimes relating to Counterfeiting of currency/Stamps stood at 53 wherein 118 persons were arrested during 2003. Of the 47,478 cases reported under Cheating, the Cyber Forgery (89) accounted for 0.2 per cent. Of the total Criminal Breach of Trust cases (13,432), the Cyber frauds (269) accounted for 2 percent. Of the Counterfeiting offences (2,055), Cyber Counterfeiting (53) offences accounted for 2.6 percent.

A total of 475 persons were arrested in the country for Cyber Crimes under IPC during 2003. Of these, 53.6 percent offenders (255) were taken into custody for offences under Criminal Breach of Trust/Fraud (Cyber) and 21.4 percent (102) for offences under 'Cyber Forgery'.

The age-wise profile of the arrested persons showed that 45 percent were in the age-group of 30-45 years, 28.5 percent of the offenders were in the age-group of 45-60 years and 11 offenders were aged 60 years and above. Gujarat reported 2 offenders who were below 18 years of age.

Fraud/Illegal gain (120) accounted for 60 per cent of the total Cyber Crime motives reported in the country. Greed/Money (15 cases) accounted for 7.5 percent of the Cyber Crimes reported. Eve-teasing and Harassment (8 cases) accounted for around 4 per cent. Cyber Suspects include Neighbours / Friends / Relatives (91), Disgrunted employees (11), Business Competitors (9), Crackers Students / Professional learners (3).

Cybercrime is not on the decline. The latest statistics show that cybercrime is actually on the rise. However, it is true that in India, cybercrime is not reported too much about. Consequently there is a false sense of complacency that cybercrime does not exist and that

society is safe from cybercrime. This is not the correct picture. The fact is that people in our country do not report cybercrimes for many reasons. Many do not want to face harassment by the police. There is also the fear of bad publicity in the media, which could hurt their reputation and standing in society. Also, it becomes extremely difficult to convince the police to register any cybercrime, because of lack of orientation and awareness about cybercrimes and their registration and handling by the police.

A recent survey indicates that for every 500 cybercrime incidents that take place, only 50 are reported to the police and out of that only one is actually registered. These figures indicate how difficult it is to convince the police to register a cybercrime. The establishment of cybercrime cells in different parts of the country was expected to boost cybercrime reporting and prosecution. However, these cells haven't quite kept up with expectations. Netizens should not be under the impression that cybercrime is vanishing and they must realize that with each passing day, cyberspace becomes a more dangerous place to be in, where criminals roam freely to execute their criminals intentions encouraged by the so-called anonymity that internet provides.

The absolutely poor rate of cyber crime conviction in the country has also not helped the cause of regulating cybercrime. There has only been few cybercrime convictions in the whole country, which can be counted on fingers. We need to ensure that we have specialized procedures for prosecution of cybercrime cases so as to tackle them on a priority basis,. This is necessary so as to win the faith of the people in the ability of the system to tackle cybercrime. We must ensure that our system provides for stringent punishment of cybercrimes and cyber criminals so that the same acts as a deterrent for others.

Threat Perceptions

UK has the largest number of infected computers in the world followed by the US and China. Financial attacks are 16 events per 1000, the highest among all kinds of attacks. The US is the leading source country for attacks but this has declined. China is second and Germany is third. It is hard to determine where the attack came from originally.

The number of viruses and worm variants rose sharply to 7,360 that is a 64% increase over the previous reporting period and a 332% increase over the previous year. There are 17,500 variants of Win.32 viruses. Threats to confidential information are on the rise with 54% of

the top 50 reporting malicious code with the potential to expose such information. Phishing messages grew to 4.5 million from 1 million between July and December 2004.

Some Indian Case Studies

1. Pune Citibank MphasiS Call Center Fraud

US $ 3,50,000 from accounts of four US customers were dishonestly transferred to bogus accounts. This will give a lot of ammunition to those lobbying against outsourcing in US. Such cases happen all over the world but when it happens in India it is a serious matter and we can not ignore it. It is a case of sourcing engineering. Some employees gained the confidence of the customer and obtained their PIN numbers to commit fraud. They got these under the guise of helping the customers out of difficult situations. Highest security prevails in the call centers in India as they know that they will lose their business. There was not as much of breach of security but of sourcing engineering.

The call center employees are checked when they go in and out so they can not copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the customers.

All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced. Police has been able to prove the honesty of the call center and has frozen the accounts where the money was transferred.

There is need for a strict background check of the call center executives. However, best of background checks can not eliminate the bad elements from coming in and breaching security. We must still ensure such checks when a person is hired. There is need for a national ID and a national data base where a name can be referred to. In this case preliminary investigations do not reveal that the criminals had any crime history. Customer education is very important so customers do not get taken for a ride. Most banks are guilt of not doing this.

2. Bazee.com case

CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Mumbai city police and the Delhi Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cyber crime cases and a lot of education is required.

3. State of Tamil Nadu Vs Suhas Katti

The Case of Suhas Katti is notable for the fact that the conviction was achieved successfully within a relatively quick time of 7 months from the filing of the FIR. Considering that similar cases have been pending in other states for a much longer time, the efficient handling of the case which happened to be the first case of the Chennai Cyber Crime Cell going to trial deserves a special mention.

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the *yahoo message group*. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

On 24-3-2004 Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore by citing 18 witnesses and 34 documents and material objects. The same was taken on file in C.C.NO.4680/2004. On the prosecution side 12 witnesses were examined and entire documents were marked as Exhibits.

The Defence argued that the offending mails would have been given either by ex-husband of the complainant or the complainant her self to implicate the accused as accused alleged to have turned down the request of the complainant to marry her.

Further the Defence counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved.

Ld. Additional Chief Metropolitan Magistrate, Egmore, delivered the judgement on 5-11-04 as follows:

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

The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered as the first case convicted under section 67 of Information Technology Act 2000 in India.

4. The Bank NSP Case

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "indianbarassociations" and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

5. SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra

In India's first case of cyber defamation, a Court of Delhi assumed jurisdiction over a matter where a corporate's reputation was being defamed through emails and passed an important ex-parte injunction.

In this case, the defendant Jogesh Kwatra being an employ of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory emails to the plaintiff.

On behalf of the plaintiffs it was contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature. Counsel further argued that the aim of sending the said emails was to malign the high reputation of the plaintiffs all over India and the world. He further contended that the acts of the defendant in sending the emails had resulted in invasion of legal rights of the plaintiffs. Further the defendant is under a duty not to send the aforesaid emails. It is pertinent to note that after the plaintiff company discovered the said employ could be indulging in the matter of sending abusive emails, the plaintiff terminated the services of the defendant.

After hearing detailed arguments of Counsel for Plaintiff, Hon'ble Judge of the Delhi High Court passed an ex-parte ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.

This order of Delhi High Court assumes tremendous significance as this is for the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

6. PARLIAMENT ATTACK CASE

Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analysing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13 2001, was sent to Computer Forensics Division of BPRD after computer experts at Delhi failed to trace much out of its contents.

The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal.

The emblems (of the three lions) were carefully scanned and the seal was also craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

7. Andhra Pradesh Tax Case

Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person.

The owner of a plastics firm was arrested and Rs 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days.

The accused person submitted 6,000 vouchers to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted.

It later revealed that the accused was running five businesses under the guise of one company and used fake and computerised vouchers to show sales records and save tax.

8. SONY.SAMBANDH.COM CASE

India saw its first cybercrime conviction recently. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone.
She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim.

At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim.

The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code.

The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company’s site.

The CBI recovered the colour television and the cordless head phone.

In this matter, the CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code — this being the first time that a cybercrime has been convicted.

The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year.

The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the the Indian Penal Code can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

9. Nasscom vs. Ajay Sood & Others

In a landmark judgment in the case of National Association of Software and Service Companies vs Ajay Sood & Others, delivered in March, '05, the Delhi High Court declared `phishing' on the internet to be an illegal act, entailing an injunction and recovery of damages.

Elaborating on the concept of 'phishing', in order to lay down a precedent in India, the court stated that it is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party's advantage. court also stated, by way of an example, that typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.

The Delhi HC stated that even though there is no specific legislation in India to penalise phishing, it held phishing to be an illegal act by defining it under Indian law as "a

misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused." The court held the act of phishing as passing off and tarnishing the plaintiff's image.

The plaintiff in this case was the National Association of Software and Service Companies (Nasscom), India's premier software association.

The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of head-hunting, the defendants composed and sent e-mails to third parties in the name of Nasscom. The high court recognised the trademark rights of the plaintiff and passed an ex-parte ad-interim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associates or a part of Nasscom.

The court appointed a commission to conduct a search at the defendants' premises. Two hard disks of the computers from which the fraudulent e-mails were sent by the defendants to various parties were taken into custody by the local commissioner appointed by the court. The offending e-mails were then downloaded from the hard disks and presented as evidence in court.

During the progress of the case, it became clear that the defendants in whose names the offending e-mails were sent were fictitious identities created by an employee on defendants' instructions, to avoid recognition and legal action. On discovery of this fraudulent act, the fictitious names were deleted from the array of parties as defendants in the case. Subsequently, the defendants admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. The court also ordered the hard disks seized from the defendants' premises to be handed over to the plaintiff who would be the owner of the hard disks.

This case achieves clear milestones: It brings the act of “phishing” into the ambit of Indian laws even in the absence of specific legislation; It clears the misconception that there is no “damages culture” in India for violation of IP rights; This case reaffirms IP owners’ faith in the Indian judicial system’s ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.

10. Infinity e-Search BPO Case

The Gurgaon BPO fraud has created an embarrassing situation for Infinity e-Search, the company in which Mr Karan Bahree was employed.

A British newspaper had reported that one of its undercover reporters had purchased personal information of 1,000 British customers from an Indian call-center employee. However, the employee of Infinity eSearch, a New Delhi-based web designing company, who was reportedly involved in the case has denied any wrongdoing. The company has also said that it had nothing to do with the incident.

In the instant case the journalist used an intermediary, offered a job, requested for a presentation on a CD and later claimed that the CD contained some confidential data. The fact that the CD contained such data is itself not substantiated by the journalist.

In this sort of a situation we can only say that the journalist has used "Bribery" to induce a "Out of normal behavior" of an employee. This is not observation of a fact but creating a factual incident by intervention. Investigation is still on in this matter.

© Talwant Singh

Addl. District & Sessions Judge, Delhi

E-Mail-talwant@yahoo.com

****