CYBER LAWS & INFORMATION SECURITY ADVISORS

Cell: +91 9510122995
Tel: 079-40030031
E-mail : cyberlawadvocate@gmail.com
cyberlawcourse.ahmedabad@gmail.com

Important Cyber Law Case Studies

1.Pune Citibank MphasiS Call Center Fraud

Some ex-employees of BPO arm of MPhasiS Ltd MsourcE defrauded US Customers of Citibank to the tune of Rs 1.5 crores. It was one of those cyber crime cases that raised concerns of many kinds including the role of "Data Protection".

The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".

ITA-2000 is versatile enough to accommodate the aspects of crime not covered by ITA-2000 but covered by other statutes since any IPC offence committed with the use of "Electronic Documents" can be considered as a crime with the use of a "Written Documents". "Cheating", "Conspiracy", "Breach of Trust", etc. are therefore applicable in the above case in addition to the section in ITA-2000.

Under ITA-2000 the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damages to the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be invoked.

2.SONY.SAMBANDH.COM CASE

India saw its first cybercrime conviction in 2013. 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, according to the cybercrime case study, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless headphone. She gave her credit card number for payment and requested the products to be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency, and the transaction was 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 about 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, 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 headphone, in this one of a kind cyber fraud case. 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 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 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.

3. The Bank NSP Case

One of the leading cybercrime cases is 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 bank's 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.

4. Andhra Pradesh Tax Case

Dubious tactics of a prominent businessman, from Andhra Pradesh, were exposed after officials of the department got hold of computers, used by the accused in one of the many cyber fraud cases in India. 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 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 was revealed that all of them were made after the raids were conducted. It was 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.

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

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

Amongst the many cyber cases in India, in this case, the defendant Jogesh Kwatra being an employee 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 plaintiff, 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 plaintiff all over India and the world. He further contended that the acts of the defendant in sending the emails had resulted in an invasion of the legal rights of the plaintiff.

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 employee 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, in this **cyber fraud case in India,** the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails, either to the plaintiff 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.

This order of Delhi High Court assumes tremendous significance as this is 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 plaintiff by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

6. 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 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 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 cybercrime cases.

7. 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, making it one of the notable cyberlaw cases in India. 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 is related to the posting of obscene, defamatory and annoying message about a divorced 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 harassment through the Internet.

On 24-3-2004, a Charge Sheet was filed, u/s 67 of the 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, in this cyber crime case, that the offending emails would have been given either by the ex-husband of the complainant or the complainant herself 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 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 the IT Act 2000, and the accused is convicted and sentenced for the offence to undergo RI for 2 years, under 469 IPC, and to pay a fine of Rs.500/- and for the offence u/s 509 IPC sentenced to undergo 1 year simple imprisonment and to pay a fine of Rs.500/- and for the offence u/s 67 of the IT Act 2000 to undergo RI for 2 years and to pay a fine of Rs.4000/-. All sentences to run concurrently."

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

8. 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. A **cybercrime case study** has been conducted on the same.

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.

The 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 penalize 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 email 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 headhunting and recruitment. In order to obtain personal data, which they could use for purposes of headhunting, the defendants composed and sent emails 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 associated with 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 emails were then downloaded from the hard disks and presented as evidence in court.

During the progress of the cyberlaw case in India, 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, fictitious names were deleted from the array of parties as defendants in the case.

Subsequently, defendants admitted to 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.

9. Cyber Attack on Cosmos Bank

In August 2018, the Pune branch of Cosmos bank was drained of Rs 94 crores, in an extremely bold cyber attack. By hacking into the main server, the thieves were able to transfer the money to a bank in Hong Kong. Along with this, the hackers made their way into the ATM server, to gain details of various VISA and Rupay debit cards.

The switching system i.e. the link between the centralized system and the payment gateway was attacked, meaning neither the bank nor the account holders caught wind of the money being transferred.

According to the cybercrime case study internationally, a total of 14,000 transactions were carried out, spanning across 28 countries using 450 cards. Nationally, 2,800 transactions using 400 cards were carried out.

This was one of its kinds, and in fact, the first malware attack that stopped all communication between the bank and the payment gateway.

10. Tampering with Computer Source Documents

In a case of manipulation, Tata Indicom employees were taken into custody in relation to the tampering of the electronic 32-bit number (ESN) that is programmed into cell phones. The theft was for Reliance Intercom. In a verdict on a later date, the court said that since the source code was manipulated, it calls the use of Section 65 under the Information Technology Act.

11. BSNL, Unauthorized Access

In a leading cybercrime case, the Joint Academic Network (JANET) was hacked by the accused, after which he denied access to the authorized

users by changing passwords along with deleting and adding files. Making it look like he was authorized personnel, he made changes in the BSNL computer database in their internet users' accounts.

When the CBI carried out investigations after registering a cybercrime case against the accused, they found that the broadband Internet was being used without any authorization. The accused used to hack into the server from various cities like Chennai and Bangalore, amongst others. This investigation was carried after the Press Information Bureau, Chennai, filed a complaint.

In the verdict by the Additional Chief Metropolitan Magistrate, Egmore, Chennai, the accused from Bangalore would be sent to prison for a year and will have to pay a fine of Rs 5,000 under Section 420 IPC and Section 66 of the IT Act.

12. BPO Fraud

In another incident involving MphasiS, India, four call centre employees gained the PIN codes, from four of the MphasiS's client, Citi Group, in spite of not being authorized to do so. Various accounts were opened in Indian banks, under false names and within two months, they managed to transfer money to these accounts from Citigroup customers accounts using their PINs and other personal information.

This cyber fraud case occurred in December 2004, but it wasn't until April 2005 that the Indian police were able to identify the individuals to make an arrest. It was made possible with a tip provided by a U.S. bank when the accused tried to withdraw cash from these fake accounts. From the $426,000 that was stolen, only $230,000 were recovered.

The accused were charged under Section 43(a), unauthorized access involved to carry transactions.

13. Bomb Hoax Mail

In an email hoax, sent by a 15-year-old boy from Bangalore, the Cyber Crime Investigation Cell (CCIC) arrested him in 2009. The boy was accused of sending an email to a private news company saying, "I have planted 5 bombs in Mumbai, you have two hours to find them". The concerned authorities were contacted immediately, in relation to the cyber case in India, who traced the IP address (Internet Protocol) to Bangalore.

14. A Look-alike Website

A 9-person crime, was registered under Sections 65, 66, 66A, C and D of the Information Technology Act, along with Sections 419 and 420 of the Indian Penal Code. Under the complaint of this cyber fraud case in India, a company representative in the business of trading and distribution of petrochemicals in India and abroad had filed the report against the 9 accused of using a similar looking website to carry on the trade.

The accused ran a defamation campaign against the company, causing them crores of rupees of loss from their customers, suppliers and even producers.

15. Cyber Terrorism

Since the changes were carried out in the Information Technology Act in Mumbai, this case of cyber terrorism was its first project. A threat email had been delivered to the BSE and NSE, at 10:44 am on Monday. With the MRA Marg police and the Cyber Crime Investigation Cell (CCIC) working together on the cyber crime case, the accused has been detained. The IP address had been traced to Patna, Bihar. When checked for any personal details, two contact numbers were found, which belonged to a photo frame maker in Patna.

Personal Cases

1. Cyber Police has arrested a Husband for misusing his wife's FB account, in a cyber case in India. He hired an ethical hacker to hack into his wife's FB account so that he can find pieces of evidence regarding her bad character.
2. Using the trojan or malware, a woman's webcam was accessed to capture her private videos and posted on an illegal website. The incident came into light when the Mumbai resident appeared for an interview.
3. The cyber fraud case of duplication of a SIM card was registered with the police when a businessman from Ahmedabad caught wind of it. He registered a complaint under the cyber and financial crime since the defrauders had submitted fake documents with the mobile company to gain the businessman's personal details.
4. In a social media related cybercrime complaint, a famous Gujarati singer claimed that her photos were being used by an unknown man, saying they were married and had a child together.
5. To gain personal revenge, an ex-boyfriend, working as a software engineer, posted his ex's personal phone number on a 24*7 dating service helpline, was arrested in a leading cybercrime case.

Contact Details

Phone: 079-40030031 , +91 9510122995

Email: cyberlawcourse.ahmedabad@gmail.com
cyberlawadvocate@gmail.com

Address

2nd Floor, Asha Complex,
B/h. Navrangpura Police Station,
Navrangpura, Ahmedabad,
Gujarat, India, 380 009.

Case Studies
Awards & Recognition
Start Up Consulting
Contact Us
Blog