Case Studies as per selected IT Act Sections Related to Offences

A **contravention** is a mere violation of law or procedure, which does not result in a criminal prosecution. It may result in a civil prosecution. On the other hand, an **offence** is an act forbidden by law and made punishable by fine and /or imprisonment.

- **Section 43 – Penalty and Compensation for damage to computer, computer system, etc**
  Related Case: Mphasis BPO Fraud: 2005In December 2004, four call centre employees, working at an outsourcing facility operated by MphasiS in India, obtained PIN codes from four customers of MphasiS' client, Citi Group. These employees were not authorized to obtain the PINs. In association with others, the call centre employees opened new accounts at Indian banks using false identities. Within two months, they used the PINs and account information gleaned during their employment at MphasiS to transfer money from the bank accounts of CitiGroup customers to the new accounts at Indian banks.
  By April 2005, the Indian police had tipped off to the scam by a U.S. bank, and quickly identified the individuals involved in the scam. Arrests were made when those individuals attempted to withdraw cash from the falsified accounts, $426,000 was stolen; the amount recovered was $230,000.
  Verdict: *Court held that Section 43(a) was applicable here due to the nature of unauthorized access involved to commit transactions.*

- **Section 65 – Tampering with Computer Source Documents**
  Related Case: Syed Asifuddin and Ors. Vs. The State of Andhra PradeshIn this case, Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones theft were exclusively franchised to Reliance Infocomm.
  Verdict: *Court held that tampering with source code invokes Section 65 of the Information Technology Act.*

- **Section 66 – Computer Related offenses**
  Related Case: Kumar v/s Whiteley In this case the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users.Investigations had revealed that Kumar was logging on to the BSNL

broadband Internet connection as if he was the authorized genuine user and 'made alteration in the computer database pertaining to broadband Internet user accounts' of the subscribers.The CBI had registered a cyber crime case against Kumar and carried out investigations on the basis of a complaint by the Press Information Bureau, Chennai, which detected the unauthorised use of broadband Internet. The complaint also stated that the subscribers had incurred a loss of Rs 38,248 due to Kumar's wrongful act. He used to 'hack' sites from Bangalore, Chennai and other cities too, they said.
Verdict: *The Additional Chief Metropolitan Magistrate, Egmore, Chennai, sentenced N G Arun Kumar, the techie from Bangalore to undergo a rigorous imprisonment for one year with a fine of Rs 5,000 under section 420 IPC (cheating) and Section 66 of IT Act (Computer related Offense).*

- **Section 66A – Punishment for sending offensive messages through communication service**
  - ***Relevant Case #1: Fake profile of President posted by imposter*** On September 9, 2010, the imposter made a fake profile in the name of the Hon'ble President Pratibha Devi Patil. A complaint was made from Additional Controller, President Household, President Secretariat regarding the four fake profiles created in the name of Hon'ble President on social networking website, Facebook.The said complaint stated that president house has nothing to do with the facebook and the fake profile is misleading the general public. The First Information Report Under Sections 469 IPC and 66A Information Technology Act, 2000 was registered based on the said complaint at the police station, Economic Offences Wing, the elite wing of Delhi Police which specializes in investigating economic crimes including cyber offences.
  - ***Relevant Case #2: Bomb Hoax mail*** In 2009, a 15-year-old Bangalore teenager was arrested by the cyber crime investigation cell (CCIC) of the city crime branch for allegedly sending a hoax e-mail to a private news channel. In the e-mail, he claimed to have planted five bombs in Mumbai, challenging the police to find them before it was too late. At around 1p.m. on May 25, the news channel received an e-mail that read: "I have planted five bombs in Mumbai; you have two hours to find it." The police, who were alerted immediately, traced the Internet Protocol (IP) address to Vijay Nagar in Bangalore. The Internet service provider for the account was BSNL, said officials.

- **Section 66C – Punishment for identity theft**
  Relevant Cases:
  - The CEO of an identity theft protection company, Lifelock, Todd Davis's social security number was exposed by Matt Lauer on NBC's Today Show. Davis' identity was used to obtain a $500 cash advance loan.
  - Li Ming, a graduate student at West Chester University of Pennsylvania faked his own death, complete with a forged obituary in his local paper. Nine months later, Li attempted to obtain a new driver's license with the intention of applying for new credit cards eventually.

- **Section 66D – Punishment for cheating by impersonation by using computer resource**
  Relevant Case: Sandeep Vaghese v/s State of Kerala
  A complaint filed by the representative of a Company, which was engaged in the business of trading and distribution of petrochemicals in India and overseas, a crime was registered against nine persons, alleging offenses under Sections 65, 66, 66A, C and D of the Information Technology Act along with Sections 419 and 420 of the Indian Penal Code.
  The company has a web-site in the name and and style www.jaypolychem.com' but, another web site www.jayplychem.org' was set up in the internet by first accused Samdeep Varghese @ Sam, (who was dismissed from the company) in conspiracy with other accused, including Preeti and Charanjeet Singh, who are the sister and brother-in-law of `Sam'
  Defamatory and malicious matters about the company and its directors were made available in that website. The accused sister and brother-in-law were based in Cochin and they had been acting in collusion known and unknown persons, who have collectively cheated the company and committed acts of forgery, impersonation etc.
  Two of the accused, Amardeep Singh and Rahul had visited Delhi and Cochin. The first accused and others sent e-mails from fake e-mail accounts of many of the customers, suppliers, Bank etc. to malign the name and image of the Company and its Directors. The defamation campaign run by all the said persons named above has caused immense damage to the name and reputation of the Company.
  The Company suffered losses of several crores of Rupees from producers, suppliers and customers and were unable to do business.

- **Section 66E – Punishment for violation of privacy**
  Relevant Cases:
  i. ***Jawaharlal Nehru University MMS scandal*** In a severe shock to the prestigious and renowned institute – Jawaharlal Nehru University, a pornographic MMS clip was apparently made in the campus and transmitted outside the university.Some media reports claimed that the two accused students initially tried to extort money from the girl in the video but when they failed the culprits put the video out on mobile phones, on the internet and even sold it as a CD in the blue film market.
  ii. ***Nagpur Congress leader's son MMS scandal*** On January 05, 2012 Nagpur Police arrested two engineering students, one of them a son of a Congress leader, for harassing a 16-year-old girl by circulating an MMS clip of their sexual acts. According to the Nagpur (rural) police, the girl was in a relationship with Mithilesh Gajbhiye, 19, son of Yashodha Dhanraj Gajbhiye, a zila parishad member and an influential Congress leader of Saoner region in Nagpur district.

- **Section-66F Cyber Terrorism**
  Relevant Case: The Mumbai police have registered a case of 'cyber terrorism'—the first in the state since an amendment to the Information Technology Act—where a threat email was sent to the BSE and NSE on Monday. The MRA Marg police and the Cyber Crime Investigation Cell are jointly probing the case. The suspect has been detained in this case.The police said an email challenging the security agencies to prevent a terror attack was sent by one Shahab Md with an ID sh.itaiyeb125@yahoo.in to BSE's administrative email ID corp.relations@bseindia.com at around 10.44 am on Monday.The IP address of the sender has been traced to Patna in Bihar. The ISP is Sify. The email ID was created just four minutes before the email was sent. "The sender had, while creating the new ID, given two mobile numbers in the personal details column. Both the numbers belong to a photo frame-maker in Patna,'' said an officer.
  Status: *The MRA Marg police have registered forgery for purpose of cheating, criminal intimidation cases under the IPC and a cyber-terrorism case under the IT Act.*

- **Section 67 – Punishment for publishing or transmitting obscene material in electronic form**
  Relevant Case:This case is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-mails were forwarded to the victim for information by the accused through a false e- mail account opened by him in the name of the victim. These postings resulted in annoying phone calls to the lady. Based on the lady's complaint, the police nabbed the accused.Investigation revealed that he was a known family friend of the victim and was interested in marrying her. She was married to another person, but that marriage ended in divorce and the accused started contacting her once again. On her reluctance to marry him he started harassing her through internet.
  Verdict: *The accused was found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000. He is convicted and sentenced for the offence as follows:*
    - *As per 469 of IPC he has to undergo rigorous imprisonment for 2 years and to pay fine of Rs.500/-*
    - *As per 509 of IPC he is to undergo to undergo 1 year Simple imprisonment and to pay Rs 500/-*
    - *As per Section 67 of IT Act 2000, he has to undergo for 2 years and to pay fine of Rs.4000/-*

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

- **Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form**
  Relevant Case: *Janhit Manch & Ors. v. The Union of India 10.03.2010 Public Interest Litigation:* The petition sought a blanket ban on pornographic websites. The NGO had argued that websites displaying sexually explicit content had an adverse influence, leading youth on a delinquent path.

- **Section 69 – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource**
  Relevant Case: In August 2007, Lakshmana Kailash K., a techie from Bangalore was arrested on the suspicion of having posted insulting images of Chhatrapati Shivaji, a major historical figure in the state of Maharashtra, on the

social-networking site Orkut.The police identified him based on IP address details obtained from Google and Airtel -Lakshmana's ISP. He was brought to Pune and detained for 50 days before it was discovered that the IP address provided by Airtel was erroneous. The mistake was evidently due to the fact that while requesting information from Airtel, the police had not properly specified whether the suspect had posted the content at 1:15 p.m.

Verdict: *Taking cognizance of his plight from newspaper accounts, the State Human Rights Commission subsequently ordered the company to pay Rs 2 lakh to Lakshmana as damages. The incident highlights how minor privacy violations by ISPs and intermediaries could have impacts that gravely undermine other basic human rights.*