CYBER CRIMES

Group Captain P Aanand Naidu(retd)

LAWS RELATING TO CYBER CRIME IN INDIA

- Introduction
- Jurisdiction
  - Sec.75. Act to apply for offence or contravention committed outside India
- Gender Neutral
- Special Laws

CYBER CRIMES

- Cyber Law and Cyber Crime
- Classification of Cyber Crimes
- Broadly there are two classes of cyber crimes
  - *Computer as a Weapon or a tool*
  - Computer as a target

  - Contraventions
  - Crimes

CYBER SECURITY NODAL BODIES

NCIIPC

CERT-IN

DISTINCTION BETWEEN CYBERCRIME AND CONVENTIONAL CRIME

- Cybercrime is a criminal activity in which computers or computer networks are a:
  - Tool, target, place of criminal activity
  - Electronic cracking to denial of service attacks
  - Traditional crimes in which computers or networks are used
- Expression crime
  - ”Offence" is defined in the IPC to mean as an act or omission made punishable by any law

COMPUTER ASSISTED CYBER CRIMES

- Computer is instrumental in committing the crime
- Selling:
  - Non-existent
  - Defective
  - Substandard
  - Counterfeit goods

COMPUTER ASSISTED CYBER CRIMES

- Theft of credit card data
- Bank fraud
- Fake stock shares
- intellectual property offences

- Selling obscene and prohibited sexual representations.

COMPUTER ORIENTED CYBER CRIMES

- Malicious Software: viruses, Trojans (which corrupt server)
- Cyber terrorism
- Child pornography
- Violent and extreme pornography
- Internet inspired homicides and suicides

.....COMPUTER ORIENTED CYBER CRIMES

- Worm: Self-replicating programmes, spread autonomously without a carrier. Ex. Via mail, scanning remote systems
- Trojan: installed during downloading some programme as a back ground activity causing irreparable damage
- Spyware: parasitic software-invades privacy-divulging details- through tracking cookies.

TROJAN HORSE

- Trojan horse

- Program that performs some ostensibly useful function but contains, lurking within its code, a damaging instruction set.
- Often, that instruction set will enable a remote user to assume control of a system, or will secretly introduce unwanted software into a system

PASSWORD THEFT

- Password sniffers

- Password sniffers are programs that monitor and record the names and password of Internet users as they log on to the network.
- The programs work by collecting bytes of the computer that is being monitored by the installer of the sniffer.
- When a network user types in a user name and a password, the sniffer collects the information and passes it on to the installer

CYBER HYGEINE

- Worms

- A worm is a stand-alone program that replicates itself.
- Both worms and viruses self- replicate.
- While a virus requires human action, from downloading a specific file to placing an infected disk in a computer, a worm uses a computer network to duplicate itself and does not require human activity for transmission

SOME ILLUSTRATIONS

- E -mail Cheating
- Cyber Whaling
- Phishing
- Pharming

REQUIREMENT OF GUILTY MIND FOR CYBER CRIMES

- Intention
  - Design of doing an act
  - Purpose/ design with which an act is done.
- Knowledge and belief
- Dishonest Intention
  - Sec 24 of IPC defines “Dishonestly”
  - Sec 25 of IPC defines “Fraudulently”

REQUIREMENT OF GUILTY MIND FOR CYBER CRIMES

- Law of Attempt
  - Intends to commit that particular offence
  - Making preparation with an intention to commit an offence
  - Such act must be proximate to offence.

CRIME IN CONTEXT OF CYBER CRIMES

- Punishments under IT Act
- Confiscation
- Residuary Penalty
- Non-Interference with other Punishments

LAW RELATING TO CYBER CRIME

CYBER CRIMES

- Section 65 – Tampering with computer source documents – punishment for 3 years or fine of Rs.2 lac or both.
- Case law – Syed Asifuddin Vs. State of UP – Tata Indicom Employees tampering Reliance Infocom phones.
- Section 66 – Computer related offences. This section is related to Section 43. Example hacking.
- Any person who dishonestly or fraudulently does any act referred to in Section 43.
- Dishonestly and fraudulently as defined in IPC.
- Case law – MG Arun Kumar Vs. Whilteley - A case of misuse of BSNL Broadband Internet connection.
- Section 66A – Sending offensive message from any communication device. Section declared void by the Apex Court in Shreya Singhal Vs. UOI

CYBER CRIMES

- Section 66B – Dishonestly receiving or retaining any computer resource or communication device – imprisonment upto 3 years or fine upto Rs.1 lac or both. Example, purchasing stolen computer or cell phone.
- Section 66C – Theft of identity – imprisonment upto 3 years and fine upto Rs.1 lac. Example, cloning of ATM cards. Case law – Vinod Kaushik Vs. Madhvika Joshi – unauthorized gaining access to the emails of husband and father-in-law
- Most of the financial frauds are covered under this Act.
- Section 66D – Cheating by personation – imprisonment upto 3 years and fine upto Rs.1 lac. Example, online fraud cases, representation as businessman, claiming of lottery amount, claiming of ancestral property, etc.
- Section 66E – Violating privacy – intentionally knowingly captures, publishes or transmits the image of a private area of any person without his or her consent under circumstances violating the privacy of that person - Imprisonment upto 3 years and fine upto Rs.1 lac.
- Obscene MMS, objectionable sms are covered under this. Case law – JNU MMS scandal and Mandi Engineering College MMS scandal.

CYBER CRIMES

- Section 66F – Cyber Terrorism – Life imprisonment; Intent to threaten the unity, integrity, security or sovereignty of India or to strike terror.
- Knowingly or intentionally accesses information, data or data base where access is restricted for reasons of security of the State or foreign relations.
- Injury to interests of the sovereignty and integrity of India.
- Security of the State
- Friendly relationship with foreign nations
- Public order or decency or morality
- Contempt of Court or defamation or incitement to an offence or to the advantage of any foreign nation or group of individuals. Example, 9/11 attack of 2001, hacking Defence, Railways or any Government sites.

CYBER CRIMES

- Section 67 – Publishing or transmitting obscene material in e-form – first conviction imprisonment upto 3 years and fine upto Rs.5 lac – second or subsequent conviction imprisonment upto 5 years and fine upto Rs.10 lac. Covered under Section 292 of IPC.
- Section 67A - Publishing or transmitting material containing sexually explicit act in e-form – first conviction imprisonment upto 5 years and fine upto Rs.10 lac – second or subsequent conviction imprisonment upto 7 years and fine upto Rs.10 lac.
- Section 67B - Publishing or transmitting material depicting children in sexually explicit act in e-form – first conviction imprisonment upto 5 years and fine upto Rs.10 lac – second or subsequent conviction imprisonment upto 7 years and fine upto Rs.10 lac.
- Case law – State of Tamil Nadu Vs. Suhash Katti – case of a family friend harassing a lady for not marrying him. The case concluded in 7 months from the filing of FIR and resulted in imprisonment as well as fine.
- Publication in the interest of public is exempt

CYBER CRIMES…CONT'D

- Sections 67C, 68, 69, 69A, 69B, 70A – deal with cyber offences relating to violation of directions of government or other competent authority - Intermediaries, certifying authorities.
- Monitoring, regulating and blocking of content, encryption or decryption of content.
- Unauthorized access to a protected system, critical information infrastructure.
- Violating the directions of CERT-IN
- Offences related to digital signature and electronic signature certificates.

VARIOUS FORMS OF HACKING

- Theft of Identity
  - Sec.66B
  - Sec.66C
  - Sec.66D
  - Sec.66 read with Sec.43(b)
  - Sec.66 read with Sec.43(h)

PHISHING

- A form of identity theft.
- The word 'phishing' is commonly used to describe the offence of electronically impersonating someone else for financial gain.
- By using someone else’s login credentials to gain access to protected systems
- By the unauthorized application of someone else’s digital signature in the course of electronic contracts
- A new type of crime has emerged wherein sim cards of mobile phones have been ‘cloned

CYBER FRAUD

- Digital Signature under section 44 of the IT ACT which is not a criminal liability
- Acts of fraud through Internet can be covered through the sections of 25 and 415 of the Indian Penal Code
- Sec. 415B Cheating
- Sec. 25- Fraudulent Act: *Section 25 of I.P.C.*
- Sec.416 Cheating by Impersonation
- Secs. 417- 420 Aggravated Cheating
- Sec 71. Penalty for misrepresentation

PUBLISHING FALSE DIGITAL SIGNATURE CERTIFICATE

- The certifying authority listed in certificate has not issued
- The subscriber listed in the certificate has not accepted it
- The certificate has been revoked or suspended
- Punishment
- Publication for fraudulent purpose
- Mischief
  - Sec. 425
  - IT Act Sec 43

CYBER DEFAMATION

- IPC Section 499
  - Exceptions to the Section 499
- Sec. 79. Network service providers not to be liable in certain cases
- Cheating by Personation
  - Sec. 66D

CYBER TERRORISM

- Section 66F - Punishment for cyber terrorism
- The section is comprehensive in that sub-clause (A)

BREACH OF CONFIDENTIALITY AND PRIVACY

- Section 72
- Punishment
- Offences by Companies
  - Section 85
- Securing Access to Protected System
  - Section 70

DIRECTIONS OF CONTROLLER TO A SUBSCRIBER TO EXTEND FACILITIES TO DECRYPT INFORMATION

- Section 69 (1)
- Section 69 (2)

PUNISHMENT FOR DAMAGE TO COMPUTER SYSTEM

- Computer, computer system or computer network downloads, copies or extracts any data
- Computer data base information from such device
- Introduces or causes to be introduced any computer contaminant
- Computer virus into any device, damages or causes to be disrupts or causes disruption;
- Denies or causes the denial of access to any person authorized to access any computer
- Provides any assistance to any person to facilitate access to a computer

LIABILITY OF INTERMEDIARIES

- Internet Service Providers (ISP)
- Search engines
- DNS providers
- Web hosts
- Interactive websites
- Cyber Cafes
- Sec.79

PROCEDURAL LAW RELATING TO CYBER CRIMES

- Introduction
- Cyber Investigation
- Compoundable offences among Cyber Crimes
- Powers of Police Officers in Investigating Cyber Offence
  - Proceeding to the spot
  - Ascertainment of the facts and circumstances of the cases

PROCEDURAL LAW RELATING TO CYBER CRIMES

- Powers of Police Officers in Investigating Cyber Offence
  - Power to Confiscate: Section 76
  - Power of Arrest: Sec 80 of IT
  - Search to arrest the accused: Section 47 CrPC
  - Power to Search persons: Section 156 CrPC

POWERS OF POLICE OFFICERS IN INVESTIGATING CYBER OFFENCE

- Power to issue summons: Section 91 CrPC
- Power to require attendance of witnesses: Section 160 CrPC
- Power to issue Search Warrant: Section 93 CrPC
- Procedure for research: Sec 100 of CrPC
- Other Provisions of CrPC

BAIL IN CYBER CRIMES

OFFENCE	Cognizable or non cognizable	Bailable or Non-bailable
The offence punishable with imprisonment less than 3 years	Non cognizable	Bailable
The offence punishable with imprisonment of three years	Cognizable	Bailable
The offence punishable with imprisonment of more than three years	Cognizable	Non-Bailable

CYBER CRIME AGAINST FORMER CHIEF JUSTICE OF INDIA

- Former Chief Justice of India Mr. R.M. Lodha received an email from his friend, justice B.P. Singh
- Sought immediate help of Rs.1 lac for treatment of his cousin.
- Mail mentioned Singh was unavailable over the phone
- Justice Lodha transferred money in two transactions
- Subsequently Justice Lodha received a mail from Justice Singh and his email was hacked. A complaint was lodged.
- The accused Mr. Dinesh Mali was arrested from Udaipur by Delhi Police

CASE LAW – DR. L. PRAKASH

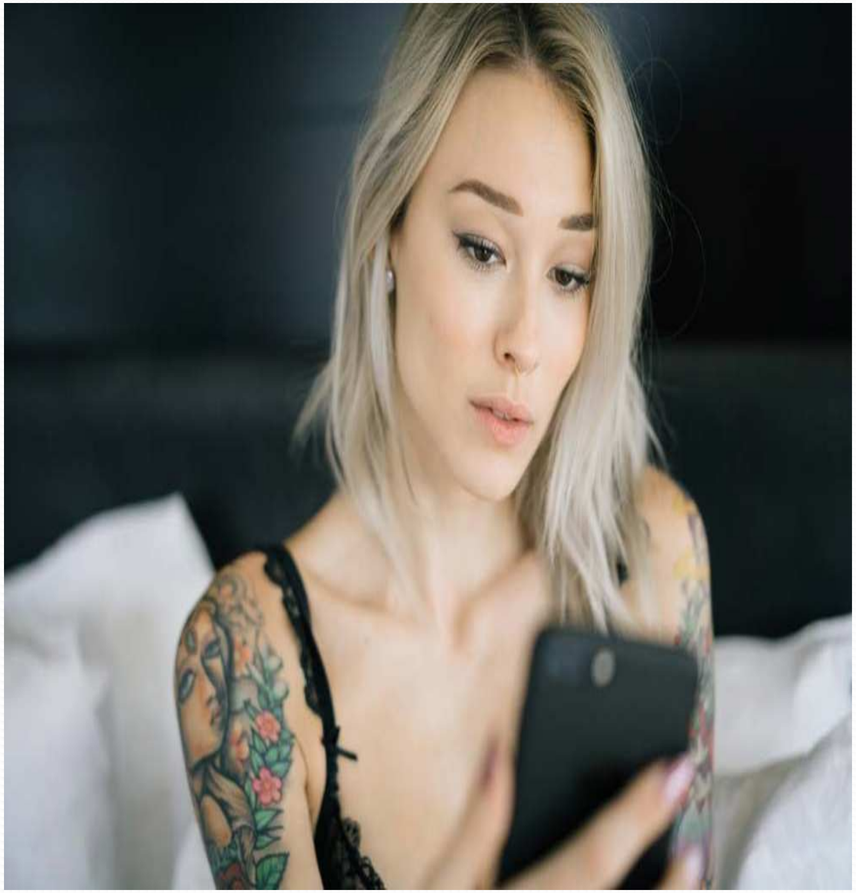
- Orthopaedic Surgeon manipulating and forcing some victims into sexual acts on camera
- His brother from US was involved
- Punished under Immoral Traffic Act, IPC, Arms Act and Indecent Representation of Women (Prevention) Act, most importantly Section 67 of IT Act.

RECENT HACK

- Twitter Hack Hits Obama, Biden, Musk in Bitcoin Scam!

- - Hacker got administrator privileges
  - Hacked verified accounts of extraordinary influencers
  - US$ 118000 (INR 86,00,000) lost in 3 hrs.

CASE STUDY



- A sends nude pictures to B; B sends them to C
- A is a minor and B is also a minor
- A is a girl and B is a boy. C is a major
- What is the offence and Provisions

Case study

- Publishing or transmitting material depicting children in sexually explicit act etc. in e-form (S. 67 B) against B read with Juvenile Justice Act

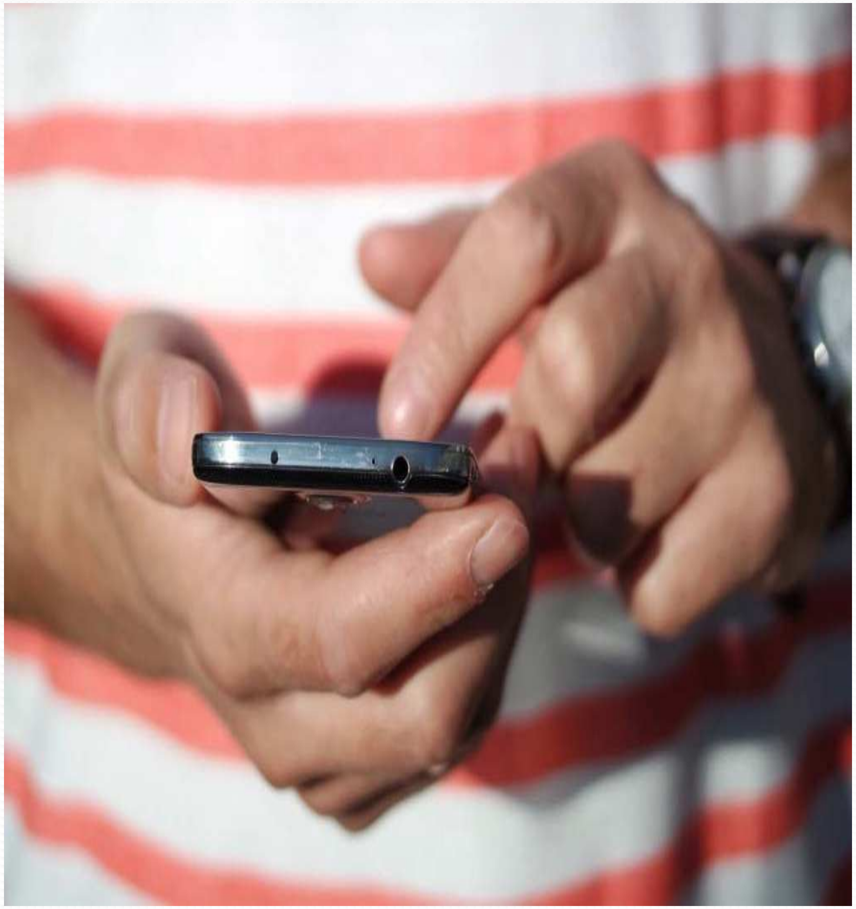
Case study

- A sends nude pictures to B
- B sends them to C
- A is major female. B is an executive in a company and a male. C is a female colleague of B
- B complains to Police
- What is the Offence and provisions

Case study

- POSH Laws applied in conjunction with Publishing or transmitting material containing sexually explicit Act in e – form
- S. 67 A
- 5 yrs and 10 lakhs for the first time or 7 yrs and 10 lakhs

CASE STUDY



- A sends SMS to B. B forwarded it to C.
- SMS contains sexually oriented message
- A is a major male. B is a female friend. C is a male colleague of B
- C wants to complain to police and seeks your advice!
- Is there an offence and provisions

CASE STUDY

- Publishing or transmitting obscene material in e- form
- S.67
- 3 yrs and 5 Lakhs for the first offence or 5 yrs and 10 Lakhs

CASE STUDY

- A is photographed by B in the presence of C and D
- Some photographs contain pictures of private parts of A
- A is a minor girl student. B, C and D are adults
- A shares those photographs with B, C and D. D sends to his friends
- Some photographs reach A’s parents
- They lodged a complaint
- A insists that she was compelled to pose for that photographs by peer pressure

CASE STUDY

- Publishing or transmitting material depicting children in sexually explicit act etc. in e- form against D
- S. 67 B
- 5 yrs and 10 lakhs for the first time or 7 years and 10 lakhs
- Violating privacy :Capturing against B, C and D
- S. 66E
- 3 yrs or 2 lakhs or both

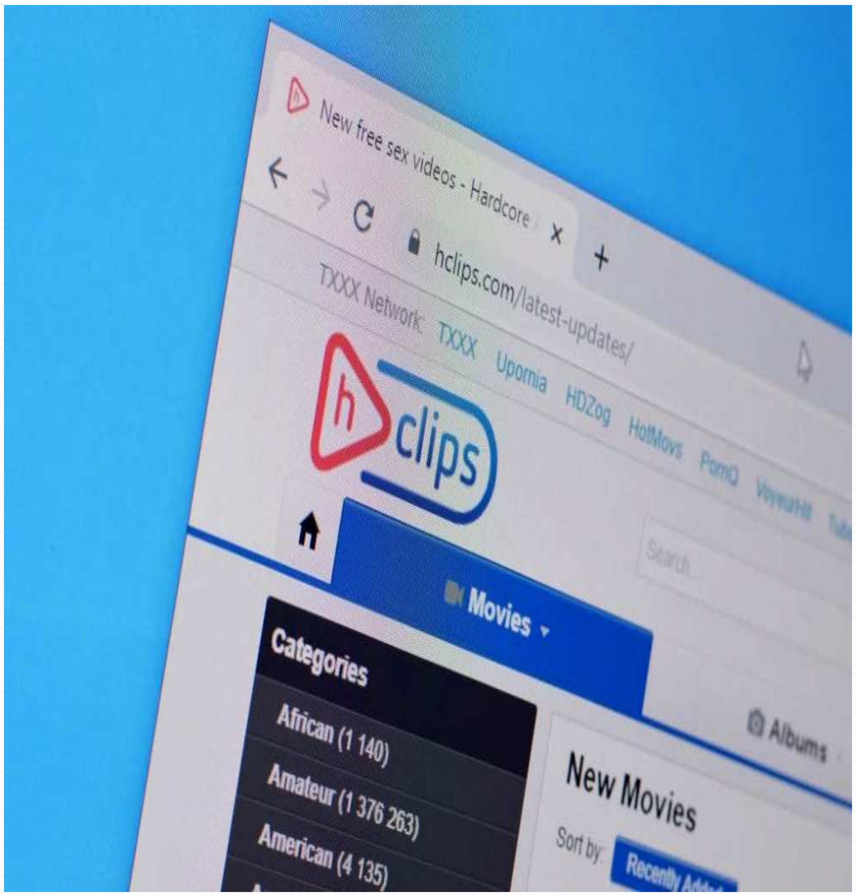
CASE STUDY

- Students of an Elite School have fun
- A organizes alcohol. Girls C and D consume liquor
- During the dance C removes her topclothes. Seeing that, B removes thetop clothes of D, despite heropposition
- E captured it on his mobile. Thatvideo goes viral
- The school management lodges acomplaint with the police based onTV news of the event
- What are the crimes and provisions

Case study

- Multiple Acts and Sections including Juvenile justice Act
- The management of PUB also responsible

CASE STUDY



- X sends a Whats App video containing sexual act involving her to Y
- Y sends that video to A
- A calls up X and demands more videos of similar nature otherwise he would report the matter to her husband
- X confides in her husband and they complain to police
- What are the offences and provision

CASE STUDY

- Y is punishable for violating privacy (transmitting)
- 3 yrs or 2 lakhs or both
- A is punishable for

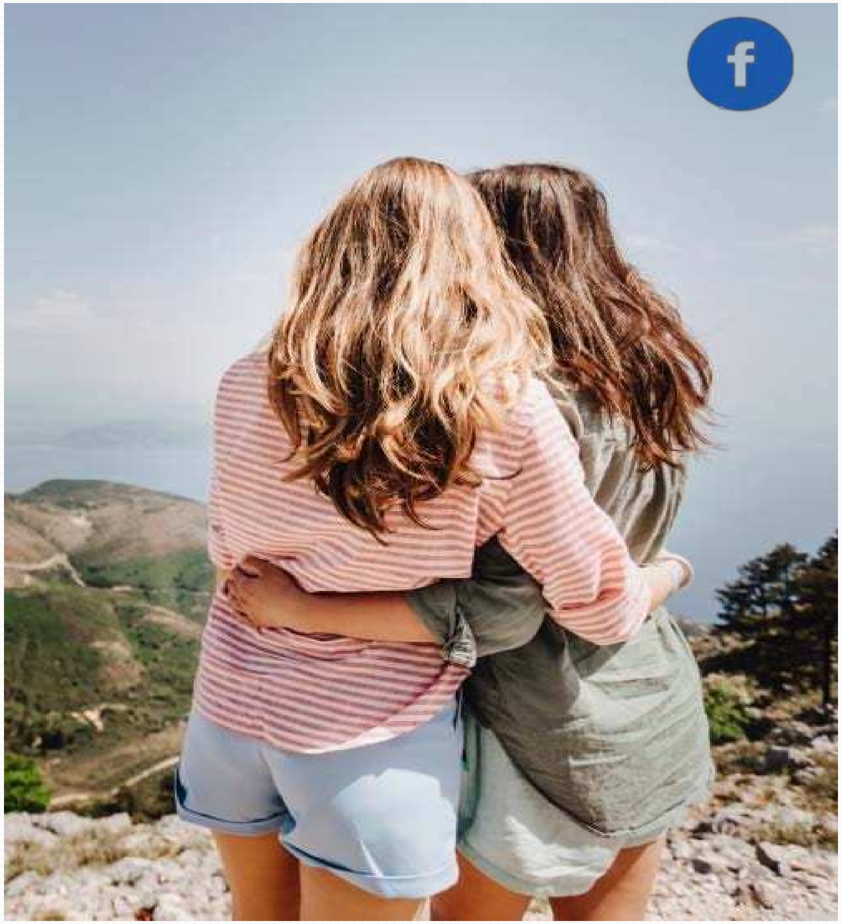
CASE STUDY

- A projecting as X, a bank officer, induces C to part with OTP for change of registered mobile number linked to the bank account
- C losses INR 50,000 due to the resultant fraud
- What are the actions by C?
- What are the liabilities of the C?
- What are the liabilities of the Bank?
- Will the liability of C change if D is an illiterate women who passed on the phone to B, a neighbor?

CASE STUDY

- RBI Circular on bank frauds applies
- Actions of C: Report (within 72 hours), complain, (in writing) FIR (cyber police and local police station
- And follow-up
- Liability of C: Subjective
- Bank can deny any liability.
- Yes. Liability of C can change, if illiterate.
- Bank has discretion

CASE STUDY



- A and B are fb girlfriends, both majors, they exchange many photographs. Some of them involving private parts, one day A informs that he is a boy and that he would like to meet B
- B refuses to meet. Thereafter, A threatens B of making the personal photos of B viral
- B complaints to police
- What are the Offences and provisions

CASE STUDY

- Cheating by personation – Section 66D, punishment – imprisonment upto 3 years and fine upto 1 lakh

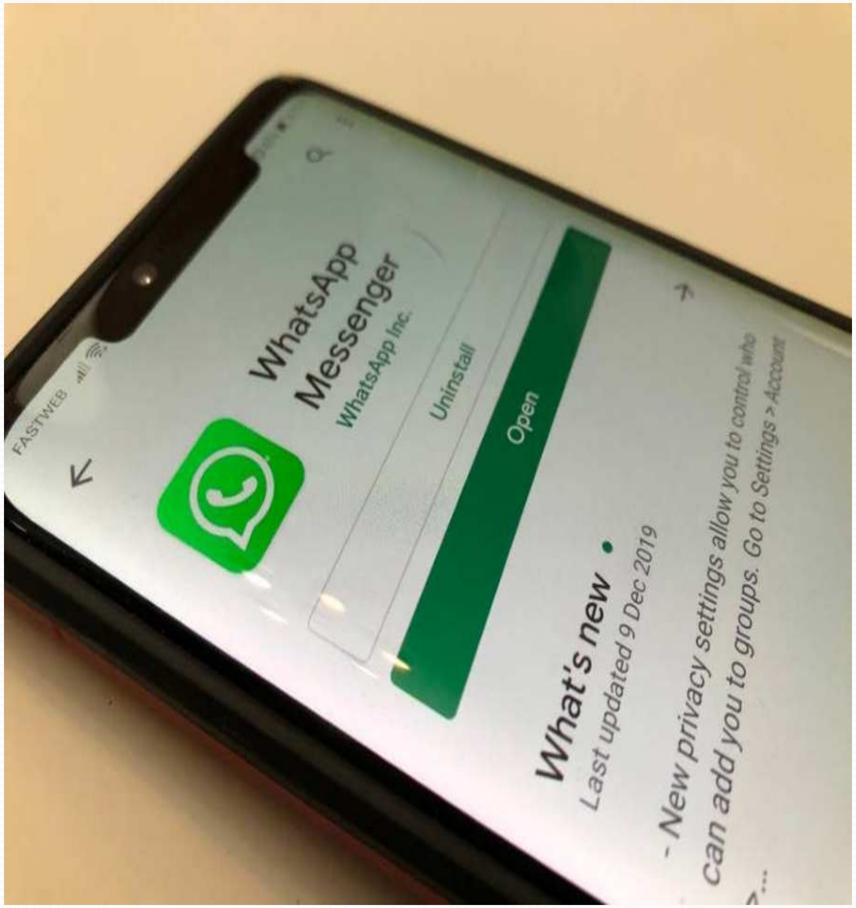
CASE STUDY

- In the above example, A proposes to have a surprize meeting with B.
- They meet in a hotel room. A declares that it's a surprize that A is not a girl
- A drugged B and makes a nude video of B
- Later B complains to police
- What are offences and provisions

CASE STUDY

- Cheating by personation – Section 66D, punishment – imprisonment upto 3 years and fine upto 1 lakh
- Violating privacy - Intentionally capturing image of private area – Section 66E, punishment – imprisonment upto 3 years and fine upto 1 lakh

CASE STUDY

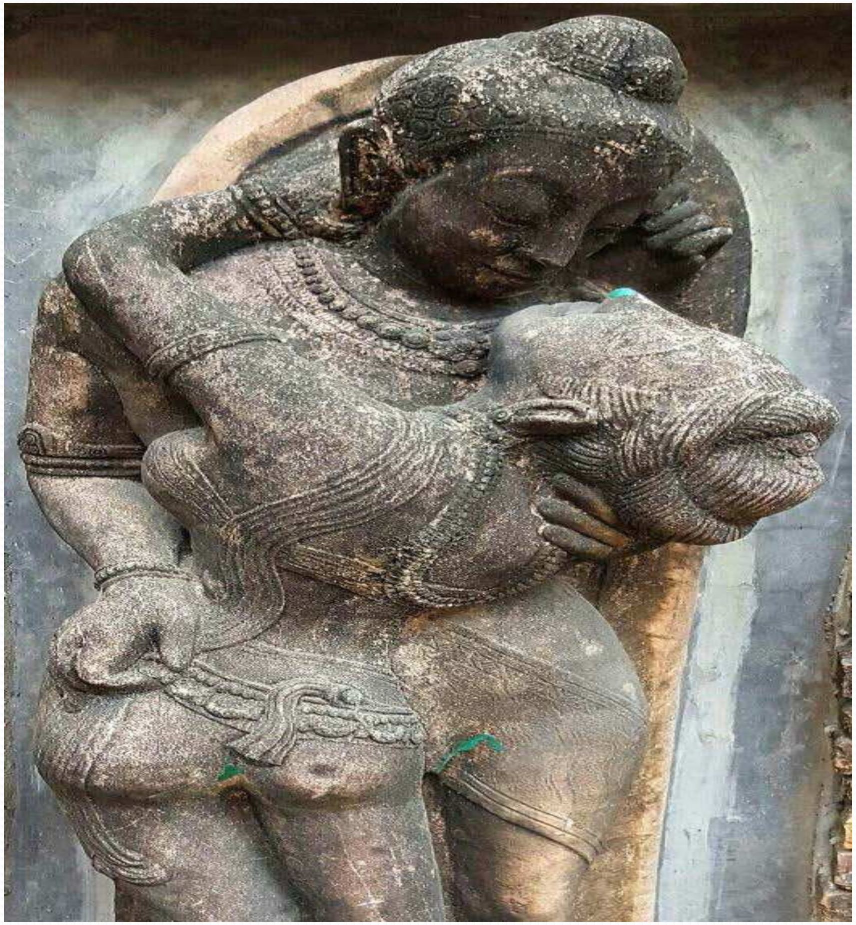


- A, a third year B-Tech student is part of a committee assisting the admission department of a college who have the data of newly admitted candidates
- On the request of cyber café owner, A supplies the contact details of all the freshers, in return for free cyber café use for 2 years
- One day, C, a female fresher gets an objectionable whatsApp message
- She complains to the college management, who lodged a police complaint.
- The whatsApp number belongs to cyber café owner
- What are the Offences and provisions

CASE STUDY

- Against - A
  - Section 43A – Failure to protect data
  - Section 43B – Copying data
  - Section 66 – Computer related offence - Punishment – imprisonment upto 3 years or fine upto 5 lakhs or both
- Against Cyber Café owner:
  - Section 66 - Computer related offence - Punishment – imprisonment upto 3 years or fine upto 5 lakhs or both

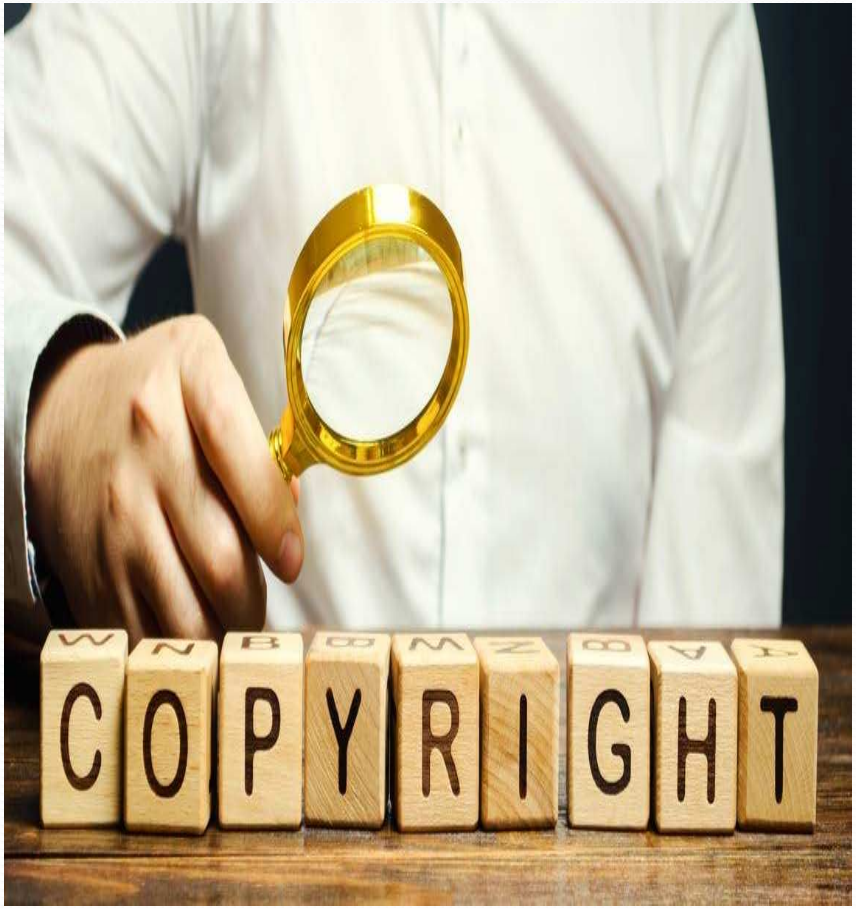
CASE STUDY



- A has written a critic on Kamasutra with many nude photos and copies of pictures taken from some temples of India
- C, an activist lodges a complaint with the police to stop the publication of the book

- Is any offence committed by A, what are the provisions

CASE STUDY

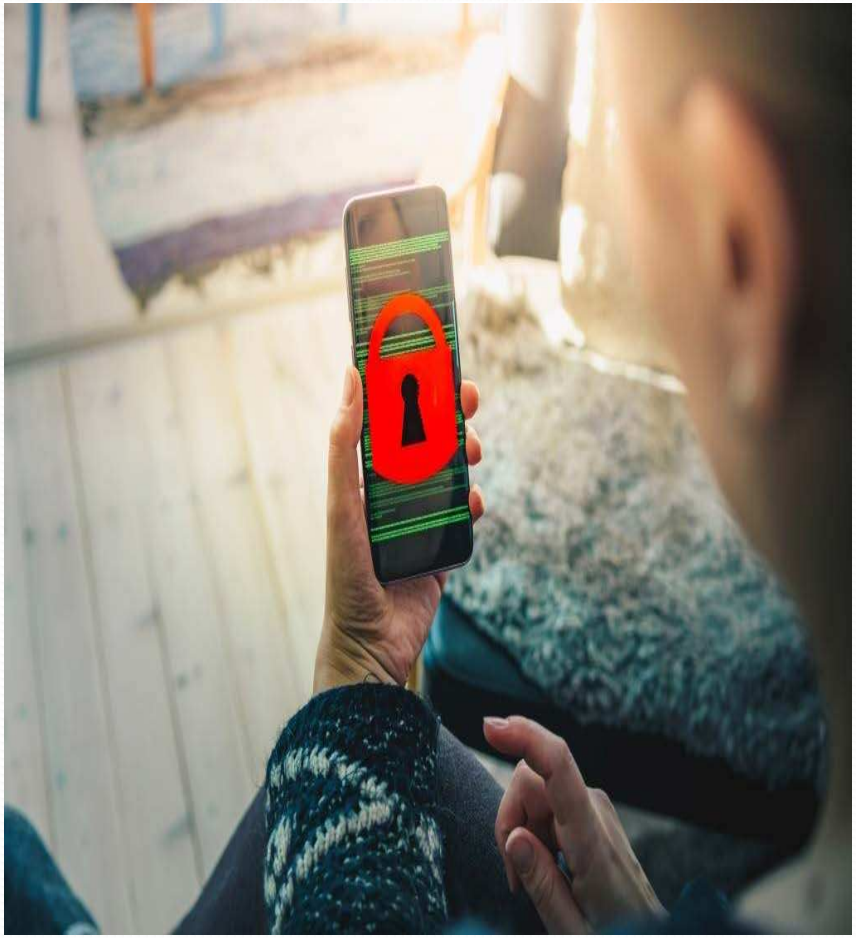


- No offence under provisio to S.67 B : publishing in public interest

CASE STUDY

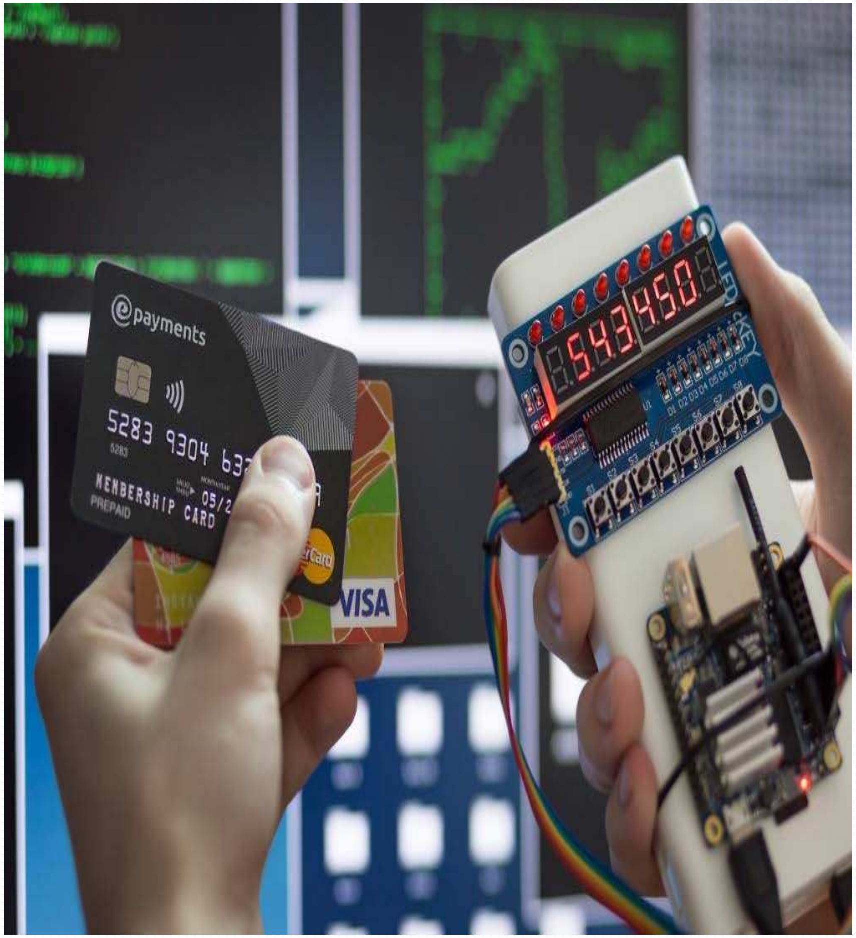
- A is wife of B. They have a marital discord
- B uploads a software to remotely monitor the communication on A's telephone
- What is the Offence and provisions

CASE STUDY



- Introduces or causes to be introduced any computer contaminant or virus
- s.43(c) and S. 66
- 3 yrs or 5 lakhs or both

CASE STUDY

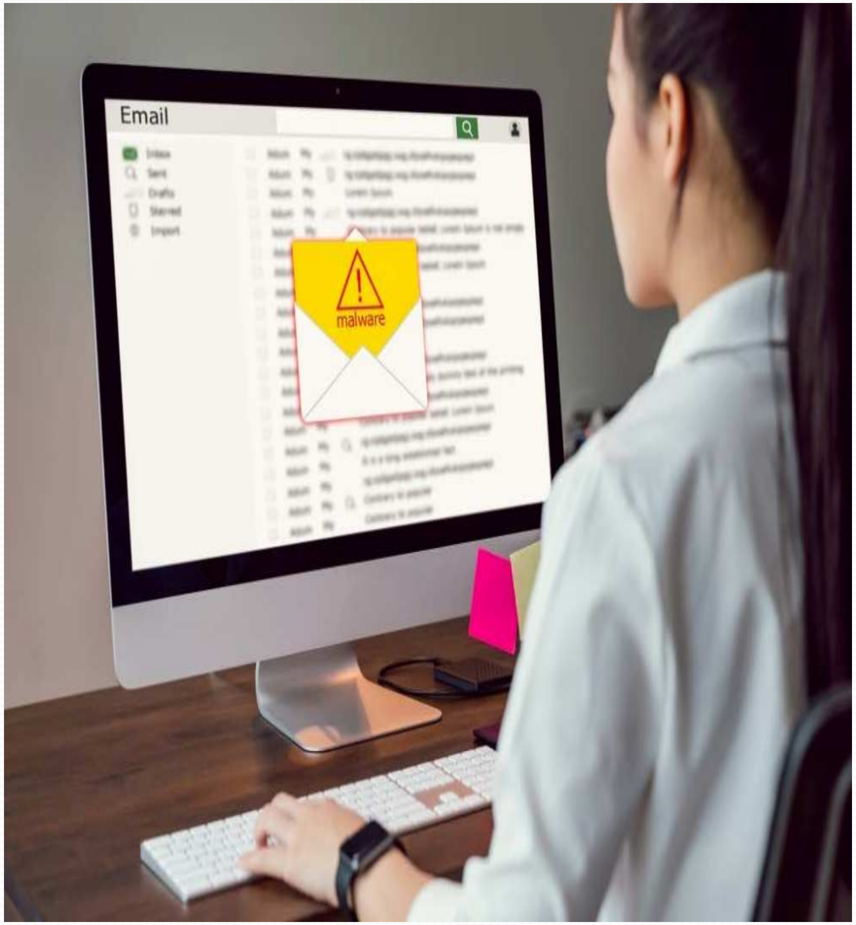


- A is husband of B
- They have marital discord and live separately
- A obtained the password to B's banking account and logged in and downloaded the summary
- B lodges a complaint to police
- What is the offence and provisions

CASE STUDY

- Computer related offences: Unauthorised access and downloading data
- S. 43 (a) and (b)
- S.66

CASE STUDY



- A sends a mail containing virus to B’s company mail
- The software system of the company malfunctions as a result
- The Company lodges a complaint
- What is the offence and provisions

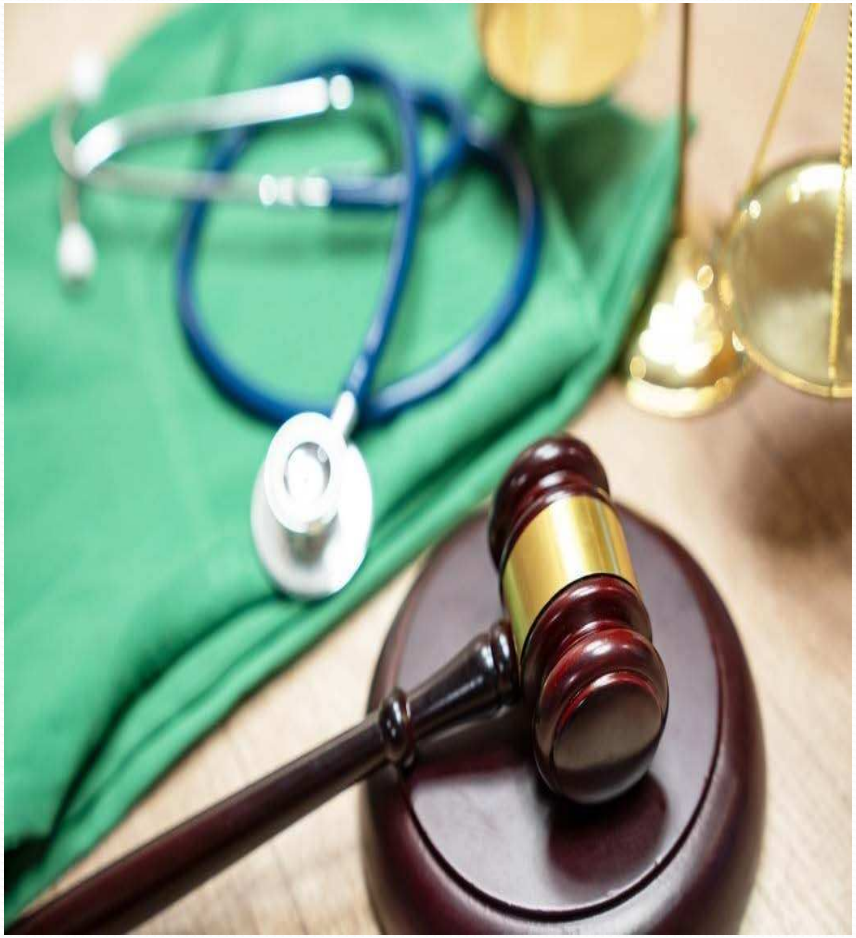
CASE STUDY

- Introduces or causes to be introduced any computer contaminant or virus
- S.43(c) and S. 66
- 3 yrs or 5 lakhs or both

CASE STUDY

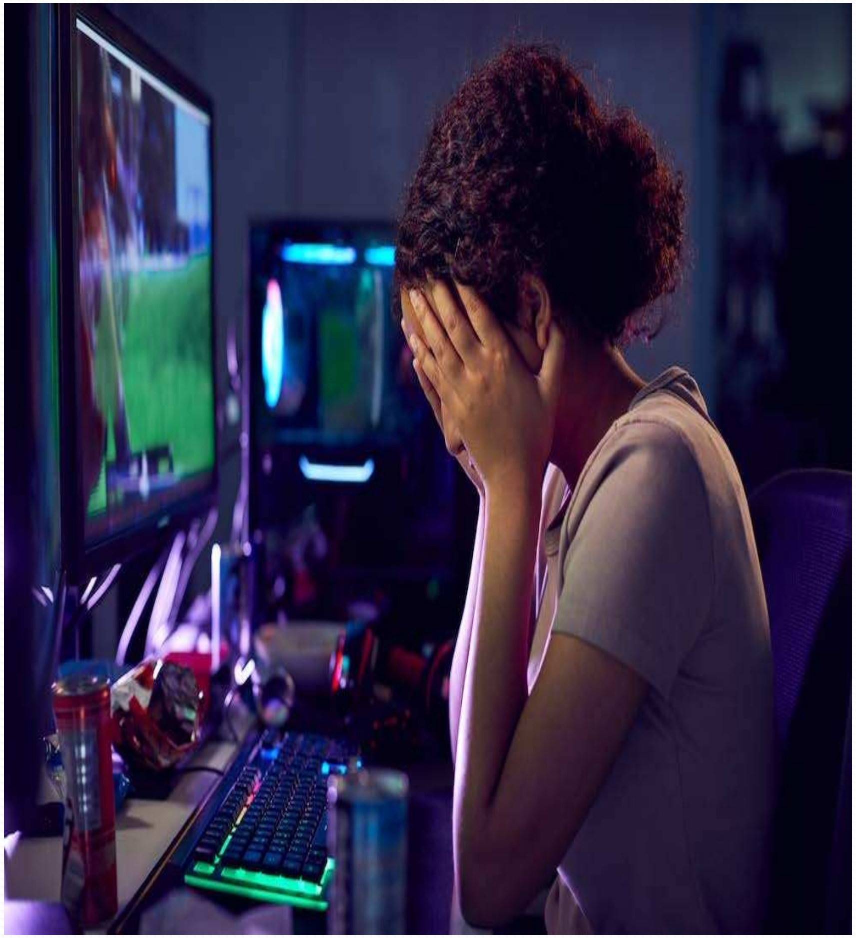
- A, a businessman asked his brother B, an employee of a software company for data related to some patients who are using their software
- B gives it to his brother
- A resorts to blackmailing the patients
- One of them lodged a complaint
- What are the offences and provisions

CASE STUDY



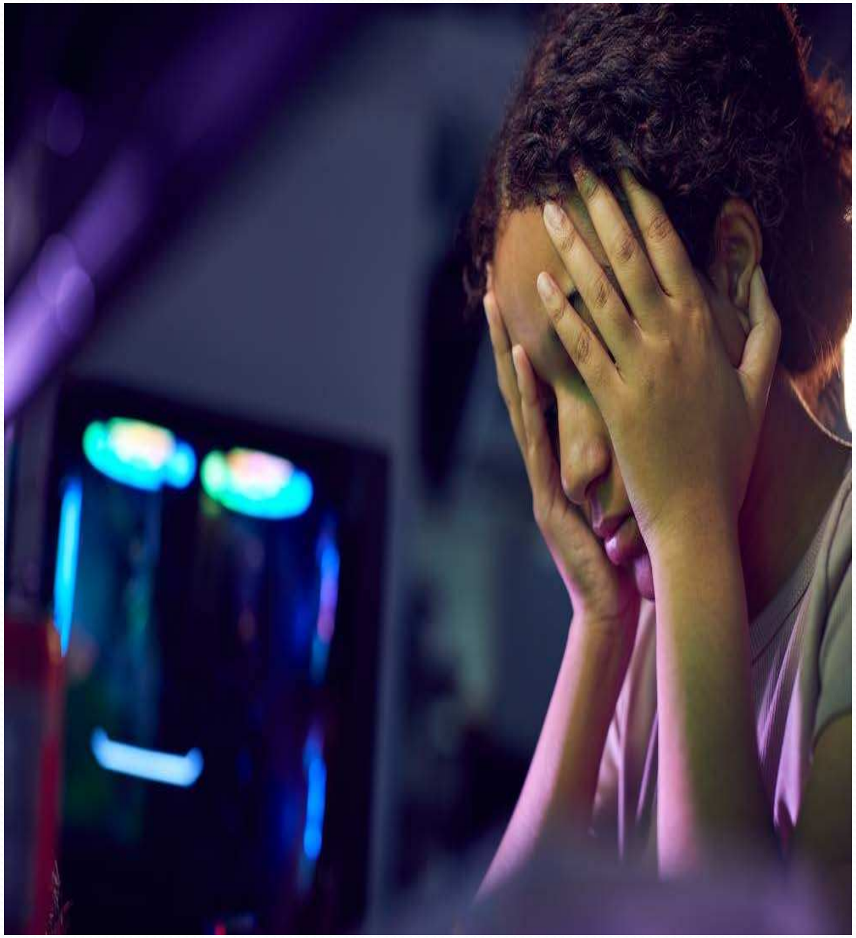
- Disclosure of info in breach of lawful contract
- s.72 A
- 3 yrs or 1 lakh or both

CASE STUDY



- A, a teen aged school girl, refuses to go to school with the symptoms of depression
- Her parents take her to the school counsellor
- A disclosed to school counsellor that she is depressed because of hate mails and messages from C and D, because of her body structure
- Is there any offence committed and what are the provisions

CASE STUDY



- Cyber Bullying
- No specific legal provision to make an offence

CASE STUDY

- A takes a laptop to B requesting him to keep it safely for 15 days. on being questioned, A informs that he bought the laptop from the black-market
- Police raids the residence of B and confiscates the laptop
- What are the offences and provisions

CASE STUDY

- Stolen Computer

- Dishonestly receiving the stolen computer resource
- S.66 B
- 3 yrs or 1 lakh or both
- Confiscation
- S. 76
- No bar for compensation or penalty

CASE STUDY

- A, a Briton, befriends B and C separately. After sometime, she informs that she is sending expensive gifts to them.
- B, a Hyderabadi, receives a call from X informing that he was calling from RGIA customs and that a consignment has come for him from UK. He is asked to pay INR 1.2 lakh as custom charges. He pays and later realises that he is defrauded.
- He complains to Police
- What are the options

ADDITIONAL READING

RBI GUIDELINES ON E-BANKING

- RBI Circulator-RBI/2017-18/15, DBR. No. LEG.BC.78/ 09.07.005 / 2017-18 Dated 6th July, 2017

SALIENT FEATURES

- Mandatory SMS alerts.
- Email alert in addition to SMS alert
- Advice costumers to notify the bank of any unauthorized bank transaction; the earlier the better.
- 24X7 access through multiple channel for reporting unauthorized transaction.
- Enable customers to instantly respond by "reply". Customer should not be required to search.

SALIENT FEATURES

- Provide direct link for lodging complaint on home page of website. Immediate response to customer acknowledging the complaint along with complaint number.
- Record time and date; this determine the liability
- No electronic transaction other than ATM cash withdrawal, if customer not providing mobile number.
- Once complaint received, bank to act and prevent further transactions

LIABILITY OF CUSTOMER

Zero liability:

- In case of ;
  - Contributing fraud/ negligence / deficiency on the part of the bank (whether reported by the customer or not)
  - Third party breach where bank and customer not responsible for the breach
- (Provided customer reports within 3 working days)

LIABILITY OF CUSTOMER (CONTD.)

- Limited liability - In case of ;
  - Loss due to negligence by customer where he shared the payment credentials, the customer will bear the entire loss till he reports.
  - Any loss after report shall be on the bank.

- In case responsibility because of the system and there is a delay of 4 to 7 working days from the customer in notifying the bank, the liability is;
  - Within 3 working days – zero
  - 4 to 7 working days – Full amount or lower of the prescribed amounts

REVERSAL TIMELINE

- The bank shall credit with 10 working days from date of notification.
- Not to wait for insurance claim.
- Bank may waive off even in case of customer negligence.

ACTIONS BY BANK

- Resolve the complaint and liability within specified time, not exceeding 90 days; payment to made.
- If, unable to resolve within 90 days, compensation as per policy.
- In case of debit card/ bank account, no loss of interest to customer.
- In case of credit card, no additional burden of interest.
- (OTP or PIN Sharing is disastrous)

SCENARIOS

- Payment service provider or the intermediaries responsible in case of outsourced ATM transactions. In this case, customer is a victim, zero liability on him, but he has to report within 3 working days
- Bank Data Base breach because of hacking. In this case, zero liability on the customer.

CASE STUDY

- Wg Cdr. Y. Prakash Rao(Retd).
  - Series of debit card credentials breached
  - Unauthorized debit card transactions take place
  - First Report within few hours
  - Bank opposes the claim
  - Customer escalates, bank denies responsibility
  - Customer reports to Air Force Police
  - Air Force Police intervenes and lodges complaints with Economic Offences Wing
  - Customer sends emails to RBI and higher management of the bank

CASE STUDY – CONTD.

- Bank refunds money and lodges FIR against unknown individuals
- After few months customer realizes that bank has opened a shadow account and retained amount equal to the transaction amount without information to the customer
- Matter reaches the court, as a result of FIR
- EOW investigation concludes without outcome.
- Court dismisses the matter.
- Customer was never informed of any progress
- Customer queries with the bank on shadow account
- Customer files RTIs – based on the replies customer files a civil case for recovery and compensation

COMPLAINT PROCEDURE

- No laid down procedure
- Timelines determine liability
- Lodge a complaint with Cyber Cell or nearest police station
- Most Cyber Cells receive complaints online or through apps
- Documents to be submitted:
  - Detailed application describing the incident
  - Self-attested government ID proof

COMPLAINT PROCEDURE

  - Copy of screen shots of the sms or email
  - Names of any suspected webpage or app used by the victim
  - Phone numbers of the fraudster, if available
  - Latest bank statement
  - Any other relevant detail / document
- Retain chats, fraudulent mails, voice recordings, phone messages in the original device, as it is
- Record in the original devise, is essential even if you made copies or forwarded to someone, because original devise will be examined in the court

COMPLAINT PROCEDURE – CONTD.

- Cyber insurances involved; hence opposition may be there
- Factual information to be mentioned
- Lodge FIR (U/s. 154 Cr.P.C)
- If police resists FIR – gets GD / DD entry made and stamped copy received
- Should block the card at the first instance - use the numbers given behind the card – don't go online to search the numbers
- Submit similar complaint to the nearest branch of your bank
- Send copy of the complaint to the RBI nearest branch. This will add weight to the complaint
- At any cost, inform within 3 working days

USEFUL TIPS

- www.cybercrime.gov.in
- It has provision for
- Crimes against women and child crime
- Anonymous complaints
- Other cyber crimes to be reported
- This portal is managed by MHA under the scheme called Indian Cyber Crime Coordination Centre (I4C)

CYBER CELLS

- Every state has a formal structure for cyber crime investigation.
- Some of the States have district level Cyber Cells
- Many Engineering Graduates who are employed in Police are deployed on these jobs
- The list of cyber cells with contact details have been sent on the WhatsApp Group

Thank You