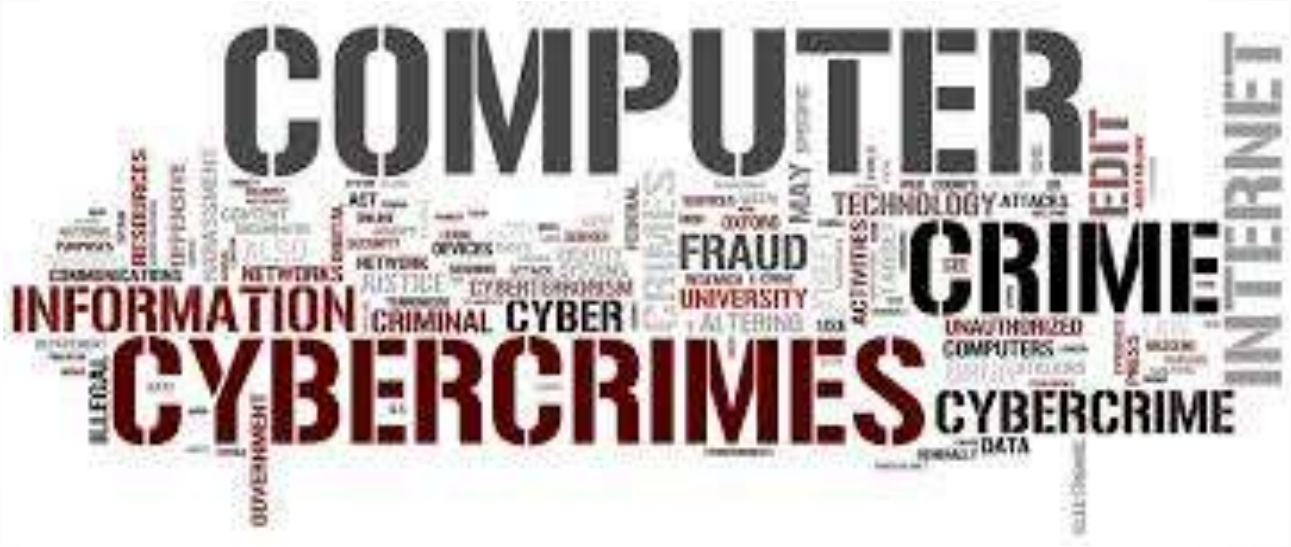
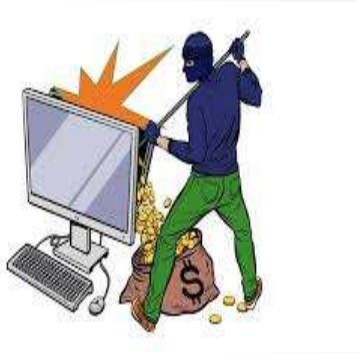
LAWS RELATING TO CYBERCRIMES: ADVANCES & BOTTLENECKS



by
Justice Raja Vijayaraghavan,
Judge
High Court of Kerala,
12/01/2020

What is CYBER CRIME?

- Any unlawful activity where –
- A computer is a TOOL,
- A computer is the TARGET, or
- BOTH



Categories

- Crime against Government
  - Cyber Terrorism, Hacking Government sites, etc.
- Crime against persons
  - Cyber Pornography, Cyber Stalking, Cyber Defamation , Business email compromise (BEC) exploits ,etc.
- Crime against Property
  - Online gambling, intellectual property infringement, Phishing, Credit Card Fraud etc.

5 Types of Cyber Criminals

The Social Engineer

The Spear Phisher

The Hacker

The Rogue Employee

The Ransom Artist

Types of Cyber Crimes

- Distributed Denial of Service Attack(DDoS)
  - Makes machine or service unavailable to intended users
- Phishing
  - Persuades users to enter personal info on an illegitimate site.
- Credit Card Fraud
  - Theft or fraud committed using credit or debit cards and obtain goods without paying
- Ransomware
  - Uses malicious software (malware) to take on data in computer and denies access. Offers to unencrypt data for money using bitcoin
- Cyber Espionage
  - Using computer networks to gain access to confidential Govt Info.

Types of Cyber Crimes (Contd.)

- Shoulder Surfing
  - Practice of surfing on the user of a cash dispensing machine to get pin
- Keylogger
  - Software installed in host machine to secretly obtain passwords
- Skimmer
  - Uses device to steal credit card data and uses it later for mischief
- Spoofing
  - One person or program masquerades as another . Email spoofing is the most popular. Seeks account details as if emanating from a known source and using the same illegal advantage is gained.
- Cyber Stalking
  - Acts of harassment or threatening behavior using internet services
- Salami Attack
  - Make insignificant alterations in accounts and swipe off money

Terrifying Cybercrime Statistics in 2018

- 780,000 records were lost per day in 2017
- Over 24,000 malicious mobile apps are blocked daily
- Healthcare industry ransomware attacks will quadruple
- More than 60% of fraud originates from mobile devices
- 300 billion passwords to be used worldwide by 2020.
- Personal data sells for as little as $0.20
- Cyber Crime to cost $6 trillion by 2021
- Source:https://www.dataconnectors.com/technews/21-terrifying-cyber-crime-statistics/

- Cybercrime generates around $1.5 trillion per year
- A hack occurs every 39 seconds
- Hackers earn around $30,000 per job, whilst their managers can make up to $2 million
- 80% of fraud are generated from mobile apps
- $1,077 is the average cash amount attackers demand
- $80 billion held in crypto currency is laundered annually.

Source:https://safeatlast.co/blog/cybercrime-statistics/#gref

NCRB DATA-2018

- During 2017-
- 56% of cyber-crime cases registered were for the motive of fraud (12,213 out of 21,796 cases)
- followed by sexual exploitation with 6.7% (1,460 cases) and
- causing disrepute with 4.6% (1,002 cases)

NCRB DATA-

Publishing material containing sexually explicit act on the internet (Sec67A)		Publishing material depicting children in a sexually explicit act (Sec67B)		Publication of obscene sexually explicit act in electronic form (not specified in the report)	
Assam	92	Uttar Pradesh	16	Uttar Pradesh	517
Karnataka	42	Assam	8	Assam	288
Telangana	35	Madhya Pradesh	7	Karnataka	157
Maharashtra	27	Himachal Pradesh	4	West Bengal	90
Odisha	24	Rajasthan/Tamil Nadu	2	Haryana	83
Total India	401	Total India	46	Total India	1768

Cyber stalking or bullying of women/children (Sec 354D IPC)

State	No. of Cases
Maharashtra	301
Andhra Pradesh	48
Haryana	27
Telangana	26
Madhya Pradesh	25
Total India	542

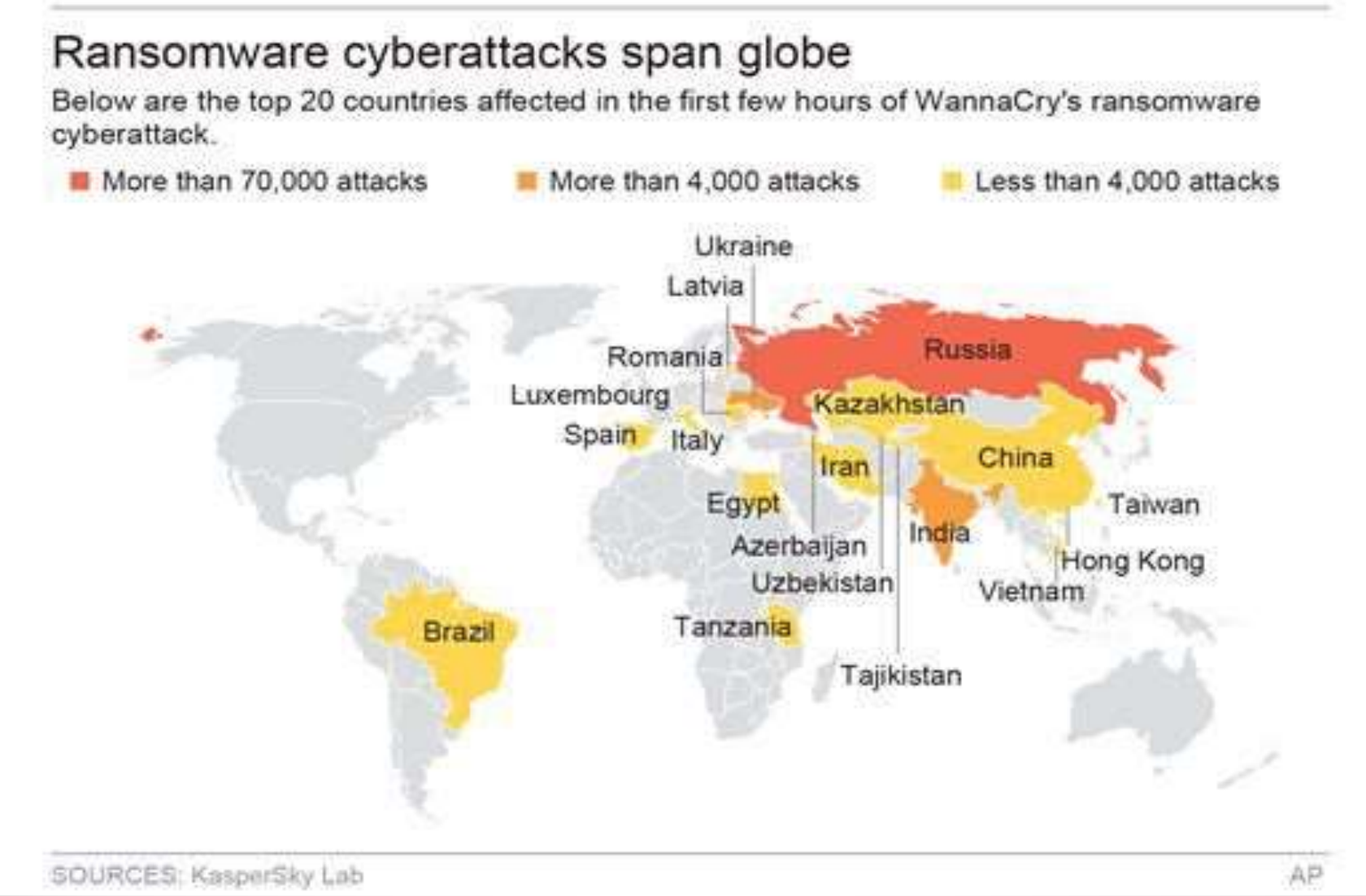
Frauds related to ATM, (OTP) under Ss.465, 468-471 IPC

ATM		Online Banking Frauds		OTP Frauds	
Maharashtra	598	Maharashtra	345	Madhya Pradesh	122
Bihar	324	Odisha	116	Andhra Pradesh	62
Odisha	168	Telangana	111	Telangana	61
Uttar Pradesh	120	Uttar Pradesh	69	Uttar Pradesh	18
Telangana	56	Gujarat	42	Rajasthan	16
India total	1543	India total	804	India total	334

Cases related to violation of privacy in cyberspace under the IT Act

- In 2017-
- Assam had the highest number of cases (60) registered for violation of privacy.
- Uttar Pradesh had 47 such cases,
- Karnataka had 38,
- Kerala had 35 and
- Maharashtra had 22 registered cases.
- The total number of such cases registered was 245.
- Source- https://www.medianama.com/2019/10/223-cybercrime-ncrb-2017/

Global Impact of Ransomware



Major Cyber Crimes of 21st Centruy

testprep training

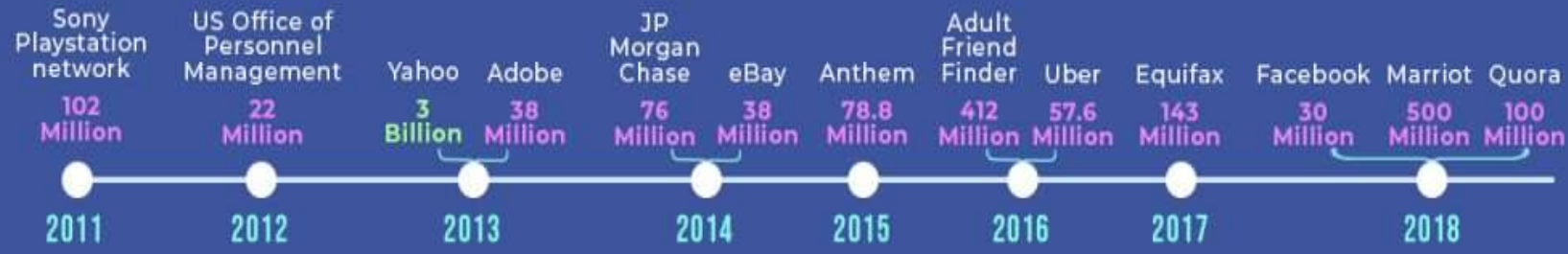
At Least 300,000 Computers & 150 Countries Were Affected By **RansomWare WannaCry** & Caused A Total Loss Of Around $4 Billion

NotPetya RansomWare Said To Be The **Most Destructive Cyber Attack**, Affected Over 80 Companies & Caused A Total Loss Of More Than $10 Billion

More Than 200,000 Malware Samples Are Being Created Everyday. 1 In Every 100 Email Contains A Malware

RansomWare Attacks Rose by More Than 30% In 2017. Globally, First Half Only Reported Around 4000 Ransomware Attacks Every Day

Biggest Data Breaches



OFFENCES

65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC.
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC

66-D	Cheating by Personation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions

67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non Bailable, Cognizable and triable by Court of JMFC

67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.

69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cybersecurity	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine	Offence is Non-Bailable, Cognizable.

70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable
71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.

72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.	Offence is Cognizable, Bailable
73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.

Compounding of Offences

As per Section 77-A of the I. T. Act, any Court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under the Act.

No offence shall be compounded if −

- *The accused is, by reason of his previous conviction, is liable to either enhanced punishment or to the punishment of different kind; OR*
- *Offence affects the socio economic conditions of the country; OR*
- *Offence has been committed against a child below the age of 18 years; OR*
- *Offence has been committed against a woman.*

The person alleged of an offence under this Act may file an application for compounding in the Court. The offence will then be pending for trial and the provisions of Sections 265-B and 265-C of Cr. P.C. shall apply.

SOME MEGA CYBER CRIMES

- UIDAI Aadhaar Software Hacked
  2018 started with a massive data breach of personal records of 1.1 Billion Indian Aadhaar cardholders. UIDAI revealed that around 210 Indian Government websites had leaked Aadhaar details of people online. Data leaked included Aadhaar, PAN and mobile numbers, bank account numbers, IFSC codes and mostly every personal information of all individual cardholders.
- If it wasn't enough shocking, anonymous sellers were selling Aadhaar information of any person for Rs.500 over Whatsapp. Also, one could get any person's Aadhaar car printout by paying an extra amount of Rs.300.

Cosmos Bank Cyber-Attack in Pune

A recent cyber-attack in India 2018 was deployed on Cosmos Bank in Pune. This daring attack shook the whole banking sector of India when hackers siphoned off Rs.94.42 crore from Cosmos Cooperative Bank Ltd. in Pune.

Hackers hacked into the bank's ATM server and took details of many visas and rupee debit cardholders. Money was wiped off while hacker gangs from around 28 countries immediately withdrew the amount as soon as they were informed.

ATM System Hacked

- Around mid-2018, Canara Bank ATM servers were targeted in a cyber-attack. Almost 20 lakh rupees were wiped off from various bank accounts. About 50 customers lost their money and the ATM details of more than 300 users were stolen.
- Hackers used skimming devices to steal information of debit cardholders. Transactions made from stolen details amounted from Rs.10,000 to the maximum amount of Rs.40,000.

SIM Swap Scam

- Two hackers from Navi Mumbai were arrested for transferring 4 crore rupees from numerous bank accounts in August 2018. The illegally transferred money from bank accounts of many individuals. By fraudulently gaining SIM card information, both attackers blocked individuals' SIM cards and by the help of fake document posts, they carried out transactions via online banking. They also tried to hack accounts of various targeted companies.

Hack Attack on Indian Healthcare Websites

- Indian-based healthcare websites became a victim of cyber-attack recently in 2019. As stated by US-based cyber-security firms, hackers broke in and invaded a leading India-based healthcare website. The hacker stole 68 lakh records of patients as well as doctors.

Attack on Kudankulam

- On 3 September 2019 the **National Cyber Co-ordination Centre**, which was set up to help the country deal with malicious cyber activities and cyber warfare, received information from a US-based cybersecurity company that a "threat actor" had breached master "domain controllers" at the Nuclear Power Corporation of India Limited's (NPCIL) Kudankulam nuclear plant.

Call Centre Fraud

- During Oct'2019, two sophisticated call centers in Kolkata, instrumental in defrauding thousands of victims in the UK alone, were shut down.

  The call centers were raided by 50 officers from the Cyber Division of Kolkata Police as part of a worldwide four-year operation conducted by the UK police and Microsoft.
- Several arrests were made.

  Source-
  https://economictimes.indiatimes.com/news/politics-and-nation/uk-india-police-shut-down-kolkata-call-centres-in-major-online-fraud-probe/articleshow/71693552.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

ISRO Attack

- ISRO attack was apparently conducted using DTrack, a type of malware, US authorities believe, is linked to the Lazarus group controlled by the North Korean government.
- Reportedly, ISRO employees accidentally installed malware on to their systems after opening phishing emails from North Korean spammers.

Challenges for Law Enforcement-CCB sleuths' mission to track down cyber criminals to Deeg, Rajasthan- returned empty handed

- The Central Crime Branch, Bangaluru sleuths trip to Rajasthan, to track down cyber criminals who were the brain behind the recent spurt in Cybercrimes in Bengaluru pertaining to QR codes, had to return back without nabbing the culprits.
- The CCB team said that the local police had not helped them in their operations, instead acted as road blocks.
- The Deeg Police also promised that they would bring the culprits and made the CCB team to wait, but later returned to say that the culprits had escaped.
- Thus months of tracking and monitoring the gang went an utter waste.
- Source- https://bangaloremirror.indiatimes.com/bangalore/crime/hunt-for-cyber-crook-vikas-proves-pointless/articleshow/73075835.cms

Legal Challenges From Social Media Platforms

- An ad hoc committee was formed by Upper House Chairman M. Venkaiah Naidu on the "alarming issue" of pornography. The 14-member panel has held several meetings and called upon various stakeholders, including the Ministry of Electronics and Information Technology (MEITY), telecom regulator TRAI and social media platforms.
- Appearing before the panel, MEITY said it faced many legal challenges from social media platforms as their servers were abroad and they "claim to be governed by laws of hosting country.
- Source- https://www.thehindu.com/news/national/platforms-like-whatsapp-not-cooperating-officials/article30374198.ece?homepage=true

Challenges for Law Enforcement

- Vijayawada Cyber Crime police serves notice to bank for negligence
- Vijayawada Cyber Crime police served notices to Infrastructure Development Finance Company (IDFC) Bank for the delay in providing data related to a crime reported two weeks ago in the city. According to Cyber Crime police station Circle Inspector (CI) K Shivaji, a cheating case as reported at Bhavanipuram police station.
- **IDFC bank took four days' time to provide the beneficiary account number. By the time Police managed to trace the accused, the money was withdrawn from the account**
- Source- https://www.newindianexpress.com/cities/vijayawada/2019/dec/19/vijayawada-cyber-crime-police-serves-notice-to-bank-for-negligence-2078128.html

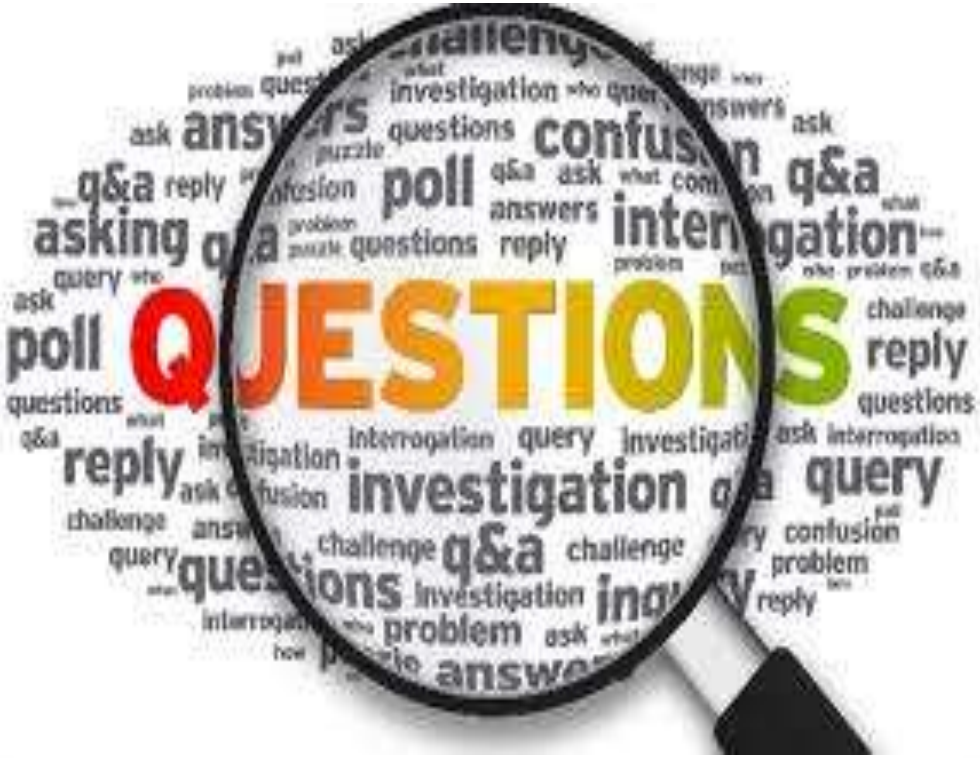
ENFORCEMENT ISSUES/BOTTLENECKS

- **Detection of Crimes** – role of victim / complainant- **Limitations due to territorial/cross border issues**.
- **Non-cooperation from ISPs and MNCs** in providing details to law enforcement agencies.
- **Anonymity**- Masking of identity
- **Lack of co-operation and intelligence sharing** guidelines between various law enforcement agencies.
- **Shortage of staff , infrastructure and expertise** to handle such cases.
- **Awareness /experience** in this area of the **police, lawyers and Judges**.
- Lack of National Guidelines regarding **search & seizure** of electronic evidence.
- **Admissibility of Digital Evidence**- Law needs to evolve and settle.

Conclusion

- There is **no straight jacket formula** as such worldwide.
- **Deadly challenges being presented by cyber criminals** across the world.
- A need for the lawmakers and all the other stakeholders to **deal with the legal and policy issues concerning cyberspace in a more effective, holistic and pragmatic manner**.
- A need to have a **comprehensive and well-defined collaboration and information sharing model among the investigating agencies.**
- Sensitivity among Judges regarding the **criticalities, subtleties and ground realities relating to cyber crimes ,investigations, and the Law**, while balancing the aspect of instilling confidence and faith of public in judiciary by their **timely** judgments.

- There is a pressing and exigent need to give out a message about the **'pernicious and far reaching impact'** of cyber-crime and to **'those who are minded to commit'** these type of offence.


QUESTIONS
poll
reply
asking
q&a
investigation
confusion
answers
questions
challenge
query
problem
interrogation