

# **Electronic Evidence: Collection, Preservation and Appreciation**

**Dr.S.Murugan IPS  
Joint Director/Inspector General of Police,  
Vigilance and Anti Corruption  
Chennai.**



# Outline of Presentation

- Cyber Crime
- Electronic Evidence
- **Acquisition, Authentication, Admissibility**
- Chain of Custody : SOP
- Digital Evidence: 2020
- Social Media
- Need of Data Protection Law
- Recent Trends in Cyber Space
- Indian Cyber Laws
- Admissibility of Evidence : Case Laws.



# Introduction

- **Technological revolution in communication and information technology.**
- **Impact of Social Media**
- **All Stake holders of judicial Justice system are to be equipped with the use of latest technology and forensic investigation techniques**
- **Public prosecutors and lawyers also require awareness on usage of Digital evidence and relevant case laws!**



# Cyber Crime

- Cyber crime is defined as a crime in which an **electronic communication Device** is the **object** of the crime, or used as a **tool / target** or used **incidental** or as a **witness** to commit an **offence**.
- Cyber criminals may use Information technology to access personal information, business trade secrets, use the internet for exploitive or malicious purposes.



# Conventional Crime Vs. Cyber Crime

## Traditional criminal techniques

**Burglary:** Breaking into a building with the intent to steal.



**Deceptive callers:** Criminals who telephone their victims and ask for their financial and/or personal identity information.



**Extortion:** Illegal use of force or one's official position or powers to obtain property, funds, or patronage.



**Fraud:** Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage.



**Identity theft:** Impersonating or presenting oneself as another in order to gain access, information, or reward.



**Child exploitation:** Criminal victimization of minors for indecent purposes such as pornography and sexual abuse.



## Cybercrime

**Hacking:** Computer or network intrusion providing unauthorized access.



**Phishing:** A high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.



**Internet extortion:** Hacking into and controlling various industry databases (or the threat of), promising to release control back to the company if funds are received or some other demand satisfied.



**Internet fraud:** A broad category of fraud schemes that use one or more components of the Internet to defraud prospective victims, conduct fraudulent transactions, or transmit fraudulent transactions to financial institutions or other parties.



**Identity theft:** The wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception, typically for economic gain.



**Child exploitation:** Using computers and networks to facilitate the criminal victimization of minors.



# Evidence...

- **Evidence is evidence is evidence!**
- **Regardless of whether the evidence is physical evidence, trace evidence, biological matter, or electronic evidence residing on a specialized device, all evidence must be treated the same**
- **Integrity must be protected at all times.**



# Types of Evidence

- **Primary Evidence**
- **Secondary Evidence**



# Electronic evidence is Primary or Secondary?

- Input: 65B IndianEvidenceAct
- Binary Equivalent:

00110110 00110101 01000010 01001001  
01101110 01100100 01101001 01100001  
01101110 01000101 01110110 01101001  
01100100 01100101 01101110 01100011  
01100101 01000001 01100011 01110100





# Evolution of Electronic Evidence

- **1984**, the FBI began to use computer evidence
- In **1991**, a new term; "Computer Forensics" was coined
- In India IT Act **2000**.

On 17th October 2000, ITA 2000 was notified and along with it the Indian Evidence Act 1872 got amended with several new sections being added to address the issue of Electronic Evidence



# Electronic Evidence

- **Evidence in digital form**
- **Data recovered from digital devices**
- **Data relating to digital devices**



# Characteristics of Electronic Evidence

- Is invisible
- Is easily altered or destroyed
- Requires precautions to prevent alteration
- Requires special tools and equipment
- Requires specialized training
- Requires expert testimony

**Digital evidence = Latent evidence**



# Where is Electronic Evidence?

- **Any kind of storage device**
  - **Computers, CD's, DVD's, floppy disks, hard drives, thumb drives**
  - **Digital cameras, memory sticks and memory/ SIM cards, PDA's, cell phones**
  - **Fax machines, answering machines, cordless phones, pagers, caller-ID, scanners, printers and copiers**
  - **CCTV**



# Type of Files

- **Audio**
- **Video**
- **Text**



# E E: A new challenge!

- Cyber crimes are being committed in cyberspace. Evidence in these crimes is almost always recorded in a digital fashion.
- **Acquisition, Authentication, and legal Admissibility** of information stored on magnetic and or any other storage media can be referred as Electronic evidence.
- Computer forensics is the application of science and engineering to the legal problem of Electronic evidence. It is a **synthesis of science and law.**



# Role of Electronic Evidence in Crime Investigation

- Evidence from tech devices continues to play a larger role in the search for justice.
- “To try to show **what happened – how it happened – when it happened,**”
- “The fact is that everything that we do has some sort of digital component,”
- “The **fit bit** along with smart watches/mobile phones
  - They know everywhere you go - the devices are always tracking information – that’s changing the game dramatically,”



# Challenges with Electronic Evidence

- Electronic evidence, by its very nature is invisible to the eye, must be developed using tools other than the human eye.
- Each step requires the use of **tools** or **knowledge**, the process must be **documented**, **reliable** and **repeatable**.
- The process itself must be understandable to the court.





# Challenges with Electronic Evidence...

- **Acquisition** of evidence is both a **legal** and **technical problem**.
- The law specifies **what** can be seized, under **what conditions**, from **whom**, and from **where** it may be seized. The determination of what a particular piece of digital evidence is, requires its **examination**.



# Documentary Evidence

- **Section 2(t) of I T Act 2000** **electronic record means;**
- **“(t) ‘electronic record’ means, “data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;”**



# Search and seizure

- **Crpc Provisions**
- **Sec 93**
- **Sec 165**
- **IT Act 2000: sec .80**
- **Independent witnesses, video, photo**

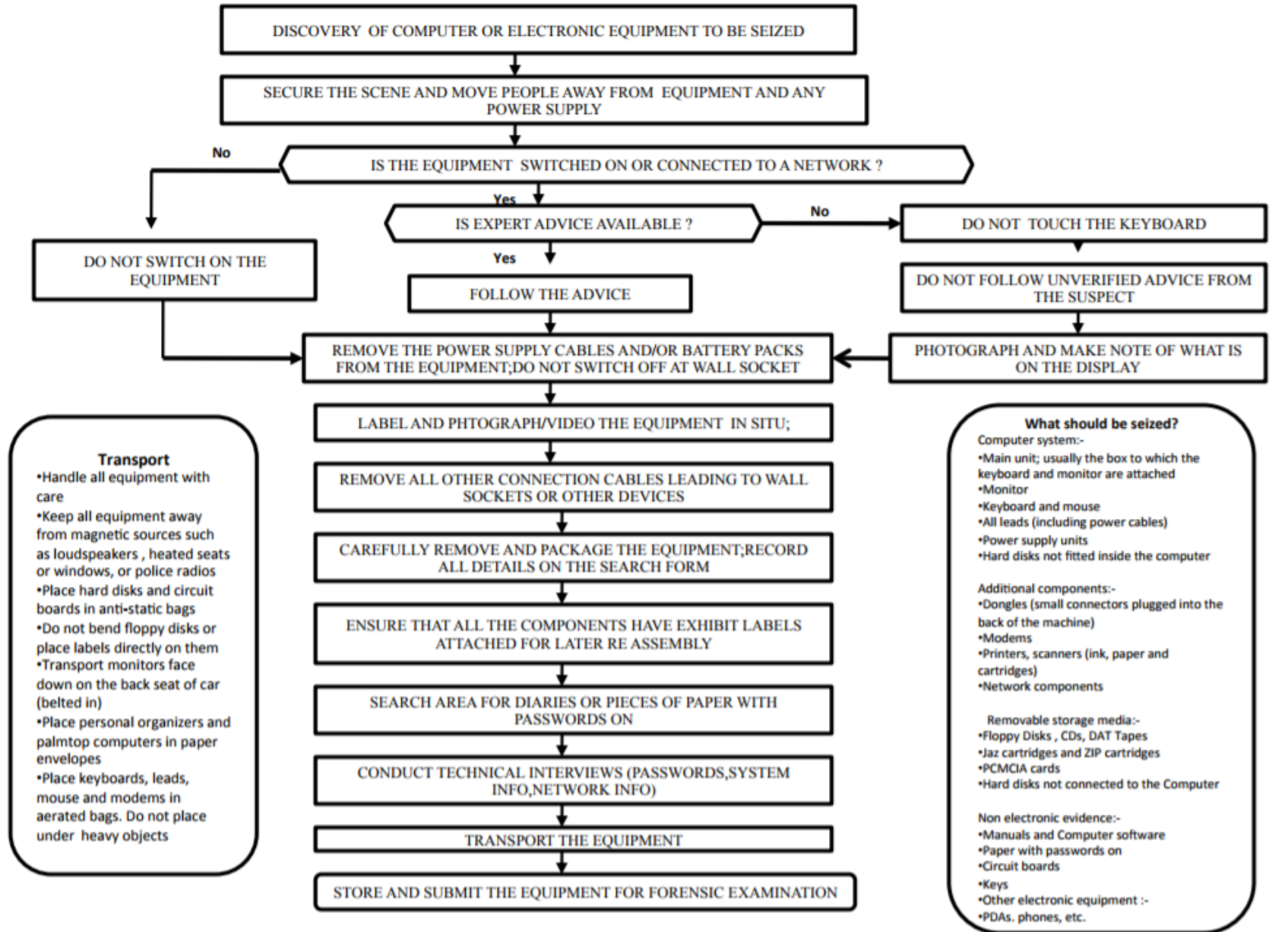


# IT ACT 2000

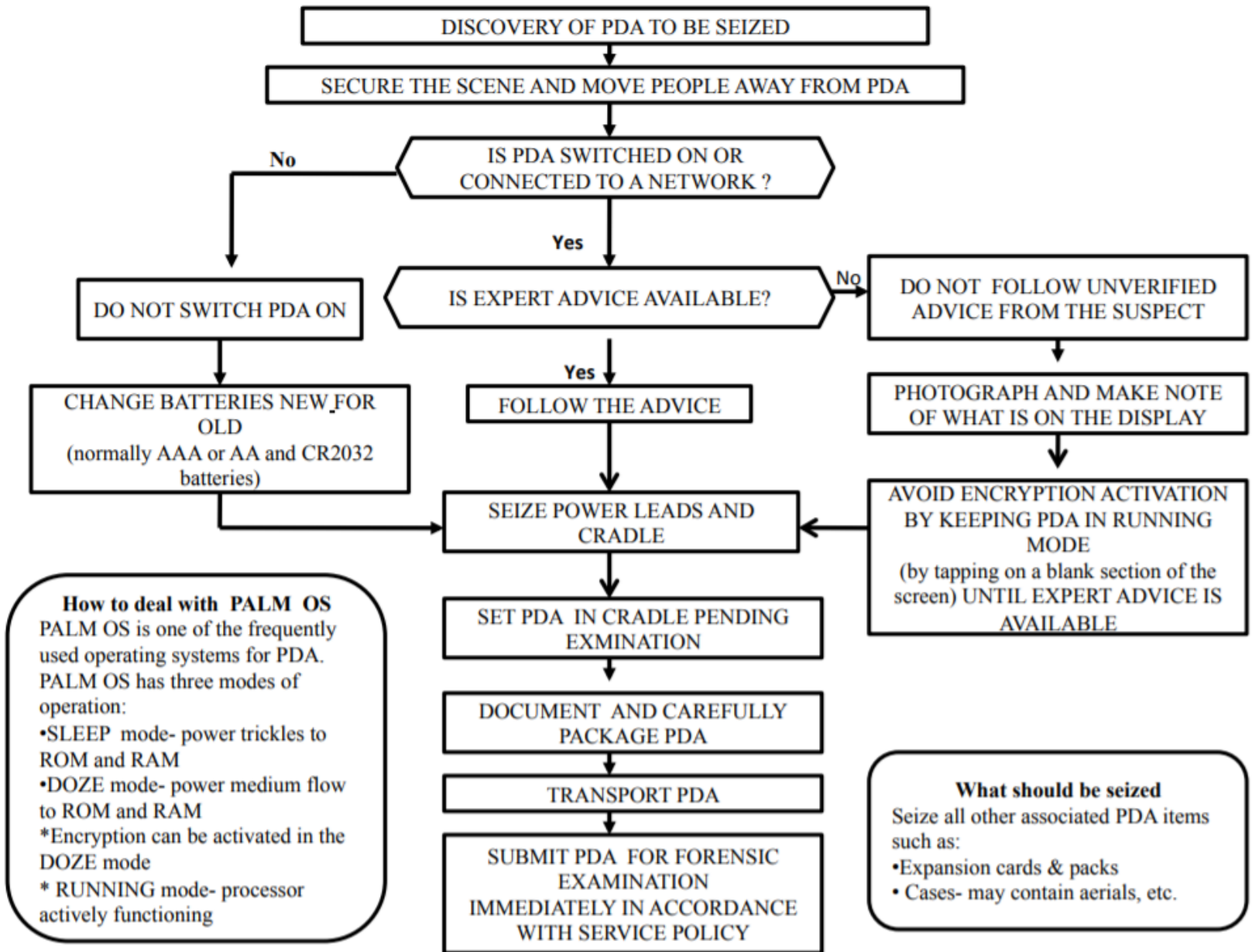
- **Sec.80. Power of police officer and other officers to enter, search, etc.**-(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, **not below the rank of a Inspector of Police**, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act.



## Seizure of Electronic equipment



## Flowchart/Pocket guide : Handheld devices (PDAs)



# Chain of custody

- **Chain of Custody – A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for any transfers**
  
- **SOP**



# Forensic Methodologies

- **Traditional Forensics**
  - Analyzing a “dead” system that has had its power cord pulled
  - Least chance of modifying data on disk, but “live” data is lost forever
- **Live Forensics (Often Incident Response)**
  - Methodology which advocates extracting “live” system data before pulling the cord to preserve memory, process, and network information that would be lost with traditional forensic approach





# Forensic copy or image?

- **Forensic image?**
- **Forensic copy?**



# Deleting a file

- **Deleting a file**
- when a file is simply deleted or erased pointers to the file are "zeroed" (i.e. alterations are made to the FAT or MFT) so that at the logical level the file does not appear to the user, but at the physical level the file data is still intact on the media and may be recovered.



# Wiping a file

- **Wiping a file**

when a file is wiped the entirety of the file is overwritten by a known or random hex character or pattern rendering it unrecoverable



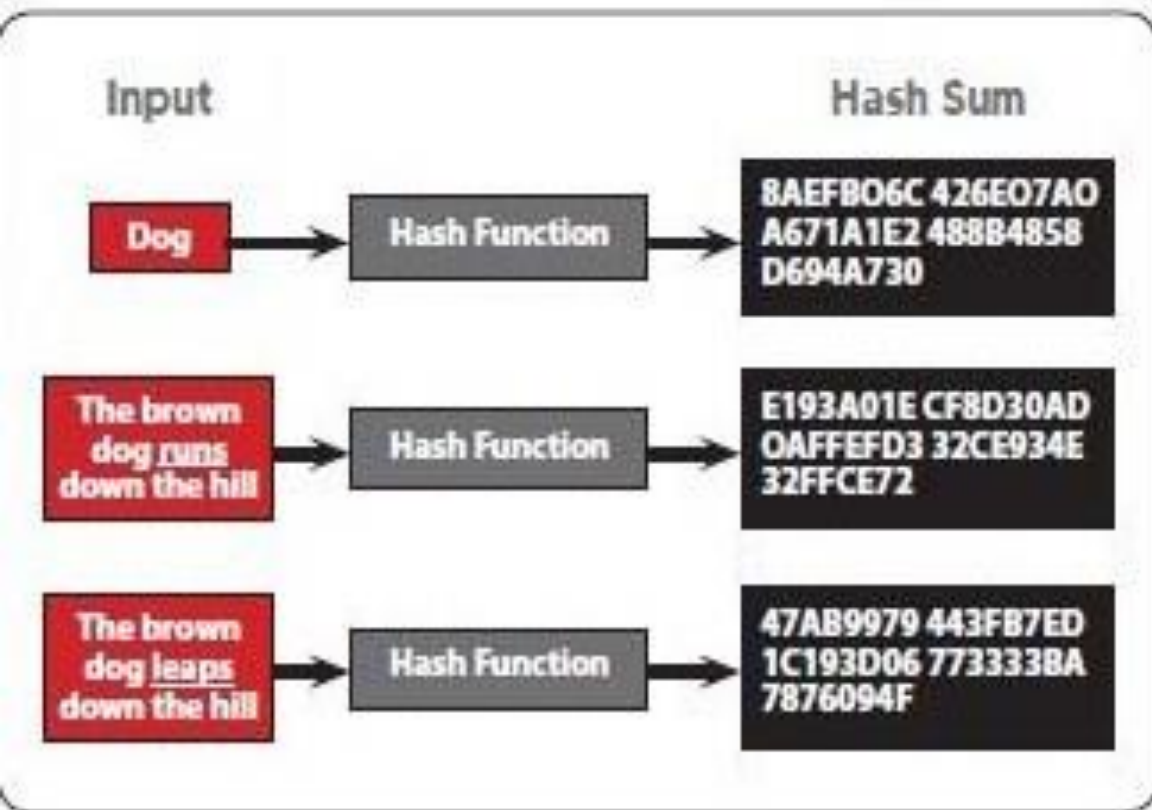
# Hash value

- A hash value is a result of a calculation (hash algorithm) that can be performed on a string of text, electronic file or entire hard drives contents.
- The result is also referred to as a checksum, hash code or hashes. Hash values are used to identify and filter duplicate files (i.e. email, attachments, and loose files) from verify that a **forensic copy or clone** was captured successfully.
- Each hashing algorithm uses a specific number of bytes to store a “thumbprint” of the contents.
  - MD5: 464668D58274A7840E264E8739884247
  - SHA-1: 4698215F643BECFF6C6F3D2BF447ACE0C067149E



# How Are Evidence Copies Verified?

The Hash Value (Thumbprint) of the Source and Copied Data are Compared

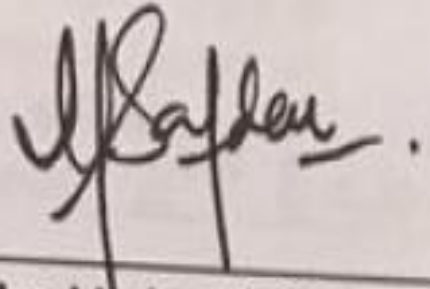


# Panama Paper Leak

- **Mariam Nawaz Sharif** purchase of high-end London property acquired through offshore companies in the British Virgin Islands.
- Documents claiming that Mariam Nawaz Sharif was only a trustee of the companies that bought the London flats, are dated February 2006, and appear to be typed in Microsoft **Calibri font**
- But the font was only made commercially available in 2007, leading to suspicions that the documents are forged.
- The Microsoft Calibri font is now a **key piece of evidence** in the case against her and the Prime Minister Nawaz Sharif after investigators found it was used in documents dated to 2006.



IN WITNESS whereof this Declaration of Trust has been duly executed on the dates and the places mentioned below.



Mrs. Mariam Safdar  
Presently at Jeddah,  
Saudi Arabia

Dated: 2<sup>nd</sup> Feb. '2006



Witness: \_\_\_\_\_

(Mrs. Mariam Safdar) 2/2/2006

This is Calibri,  
a font that was  
introduced in 2007

The document  
is dated 2006

# Provisions for the Proof of Electronic Evidence

- 65A. Special provisions as to evidence relating to electronic record
- **65B. Admissibility of electronic records**
- 67A. Proof as to digital signature
- 73A. Proof as to verification of digital signature
- 81A. Presumption as to Gazettes in electronic forms
- 85A. Presumption as to electronic agreements
- 85B. Presumption as to electronic records and digital signatures 85C. Presumption as to Digital Signature Certificates
- 85C. Presumption as to Digital Signature Certificates
- 88A. Presumption as to electronic messages
- 90A. Presumption as to electronic records five years old
- 131. Production of documents or electronic records which another person, having possession, could refuse to produce





# First myth ...

- For e.g. a yahoo mail used as Evidence...  
Some presiding officers, prosecutors and defense counsel even today call that hard disk in the yahoo server as the **“Original Evidence”** and anything else including a print out as **“Secondary”** evidence
- In electronic documents there is no “original” electronic document that can be brought into the Court and handed over to the Judge.



# Second myth...

- Many legal experts including some presiding officers, prosecutors consider that, if a Section 65B certificate is required to be submitted for an electronic document that is lying in the Yahoo Server, it has to be signed by the administrator of Yahoo.
- Section 65B certificate is a certificate provided by an **observer of an electronic document that he “experienced”** the effect of the electronic document and affirms it through the certificate and the attached set of documents in print or electronic copies.



# Social Media

- **Online Social Networking (OSN)**
- **More than 200 Social Network sites,**
- **only 15 are most popular Social networks based on number users Viz**
- **Face book, twitter whats app, imo,YouTube etc.**



# Social Media Issues

- **1.Harrasment,humilations,cyber bullying**
- **2.Use,misuse and Abuse of Art .19 of Indian Constitution: Freedom of Speech**
- **3.Sec 506, 153,A,B ,354C,D**
- **4. Netizen Rights**
- **5.Ban on Social Media**
- **6.Sec 144 Crpc**
- **7.Sec 5 of ITA 1885**



# Gaurav Sureshbhai Vyas Vs State of Gujarat 2016

- Patidar agitation led by Hardik Patel
- **Section 144 of the CrPC.**
- The Supreme Court on October 2016 upheld the power of district and state authorities all over the country to impose a limited ban on mobile Internet to prevent any law and order problems.

# Free wifi

- **All the Airports are connected with free wifi for an hour at least.**
- **Google likely to install free wifi on 140 railway stations**
- **Google not only has access to all your search records but also to metadata/search analytics from all your connected devices now.**



# Are you safe with your e mail Accounts?

**Gmail,yahoo,etc not safe**

**No social media platform is safe**

- **icloud also not safe!**
- **Use privacy settings**
- **Try to use your own e mail accounts..**



**NO  
Google  
Datacenter  
ENTRY**

Google eRuns the internet and  
Its Data Center is as guarded  
as Area 51 is. It is a high-security  
location that contains trillions  
of records of our DATA.

You cannot access it, ever.





# Data Protection Law

- Presently all our Data namely Search, Emails, Chat, Google, FB, Hotmail, Whatsapp are stored in Californian Servers ,USA Jurisdiction.
- US Foreign Intelligence Surveillance Court (FISC) with a single court order can take all Indian MPs, PMO, Home Minister, MEA's etc Email data and analyze them for leverage in Intl' Affairs. That's a severe threat, privacy intrusion.
- Not to mention even the Locations of each Citizen, Official in India can be monitored by US NSA analysts as of now with Whatsapp, Android Phones relaying data back to USA servers.
- Hence a Data Protection Law in India is the need of the hour.



# Data Protection Law

- The Govt has appointed an expert committee, headed by former Supreme Court Judge B.N. Srikrishna, to **“identify key data protection issues”** in India and recommend methods to address any potential problems.
- The committee has been appointed in view of the **“growing importance of data protection India.”**
- ***“The need to ensure growth of the digital economy while keeping personal data of citizens secure and protected is of utmost importance,”*** the circular further states, ***entrusting the committee with the task of putting together a draft data protection bill, and submitting its report “as expeditiously as possible”....***



# Aadhaar

- **E-authentication a must to curb Aadhaar frauds**
- **Now many agencies try to link your ID with Aadhaar,**
- **Don't link with the paper-based Aadhaar.**
- **Either it should be biometrically authenticated or Aadhaar OTP should be verified.**
- **Once you biometrically authenticate, then the possibility of somebody giving a fake Aadhaar or giving somebody else's Aadhaar number and linking it with a different PAN or account is ruled out.**



# Abinav srivastva case

1. UIDAI appoints entities for AUA (Authentication User Agency ) who provide certain Aadhaar enabled services by authenticating the Aadhaar card holder. They fetch information from the CIDR via ASA (Aadhaar Service Agency).
2. Accused identified vulnerabilities existing in e-hospital android app ( online reservation system for booking doctor/hospital appointments).
3. He developed his own app that would connect to e-hospital app at the backend and provide e-KYC services to the users.
4. e-KYC being provided was OTP based (only individual person having access to his registered mobile number can view the demographic information ).
5. But, the offence is related unauthorised access to AUA and providing the authentication and e-KYC API services in unauthorised manner.
6. The above is in violation of the section 29(2) of the Aadhaar Act 2016 and certain provisions of IT act 2000.



# Disclaimer...

**“This is not an official application from Ministry of Unique Identification Authority of India and is no way endorsed by the Government of India. Moreover, we don't store any of your aadhaar data on our server,. The app is well funded by ads and we don't need to reuse users aadhaar data in any form”**



# EE: 2020 Vision

- **Software will disrupt most traditional industries in the next 5-10 years.**
  - **Uber** is just a software tool, they don't own any cars, and are now the biggest taxi company in the world.
  - **Airbnb** is now the biggest hotel company in the world, although they don't own any properties.
  - In the US, young lawyers already don't get jobs. Because of **IBM Watson**, you can get legal advice (so far for more or less basic stuff) within seconds, with 90% accuracy compared with 70% accuracy when done by humans.
  - Watson already **helps nurses diagnosing cancer**, 4 times more accurate than human nurses.
  - Facebook now has a pattern recognition software that can recognize faces better than humans.



# EE: 2020 Vision...

- **Autonomous cars:** In 2018 the first self driving cars will appear for the public. Around 2020, the complete industry will start to be disrupted. You don't want to own a car anymore. You will call a car with your phone, it will show up at your location and drive you to your destination. You will not need to park it, you only pay for the driven distance and can be productive while driving.
- **Our kids will never get a driver's licence and will never own a car.**



# Zero Accident, no car parking

- **No need for huge Car Parking** 90 to 95% car parking places may be converted as parks.
- **1.2 million people die each year in car accidents worldwide.** We now have one accident every 100,000 km, with autonomous driving that will drop to one accident in 10 million km.
- That will **save a million lives each year.**





# Motor car, Insurance and Real Estate

- **Most car companies** will probably become bankrupt. Traditional car companies try the evolutionary approach and just build a better car, while tech companies (**Tesla, Apple, Google**) will do the revolutionary approach and build a computer on wheels. Many engineers from Volkswagen and Audi; are completely terrified of Tesla.
- **Insurance companies** will have massive trouble because without accidents, the insurance will become 100 cheaper. Their car insurance business model will disappear.
- **Real estate will change.** Because if you can work while you commute, people will move further away to live in a more beautiful neighborhood.



# Health

- **Health:** The Tricorder price will be announced this year. There are companies who will build a medical device (called the "**Tricorder**" from Star Trek) that works with your phone, which takes your retina scan, your blood sample and you breath into it.
- It then analyses **54 biomarkers** that will identify nearly any disease. It will be cheap, so in a few years everyone on this planet will have access to world class medical analysis, nearly for free. Goodbye, medical establishment.



# Recent Trends in Cyber Space

- **1. Ransomware**
- **2. Crpto currencies**
- **3. Dark web**



# Ransomware

- Ransomware is malware for data kidnapping, an exploit in which the attacker encrypts the victim's data and demands payment for the decryption key.
- Ransomware spreads through e-mail attachments, infected programs and compromised websites. A ransomware malware program may also be called a cryptovirus, cryptotrojan or cryptoworm.



# Bit Coin



- **A distributed, decentralized digital currency system**
- **Released by Satoshi Nakamoto 2008**
- **Effectively a bank run by an ad hoc network**
  - **Digital checks**
  - **A distributed transaction log**

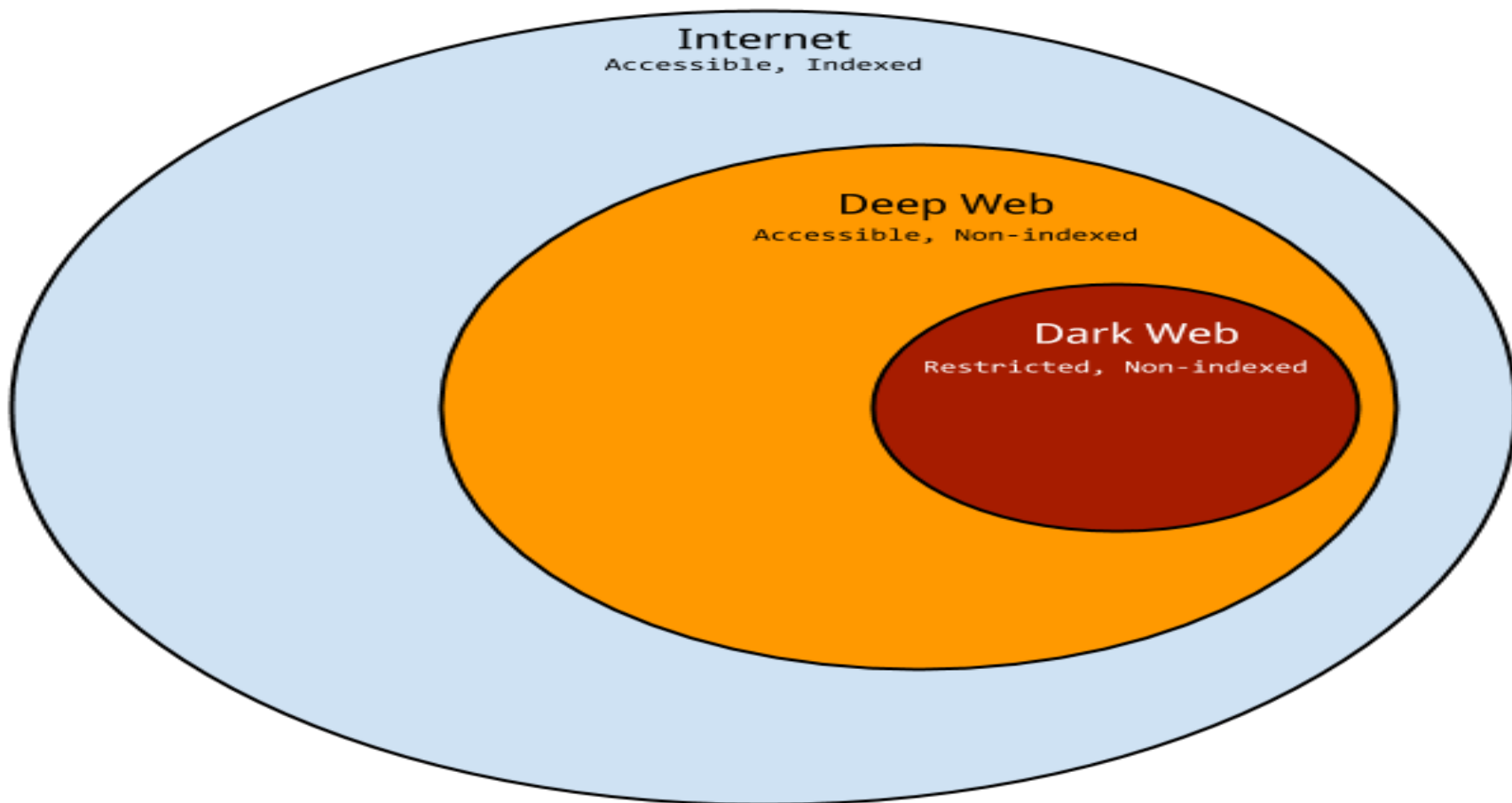


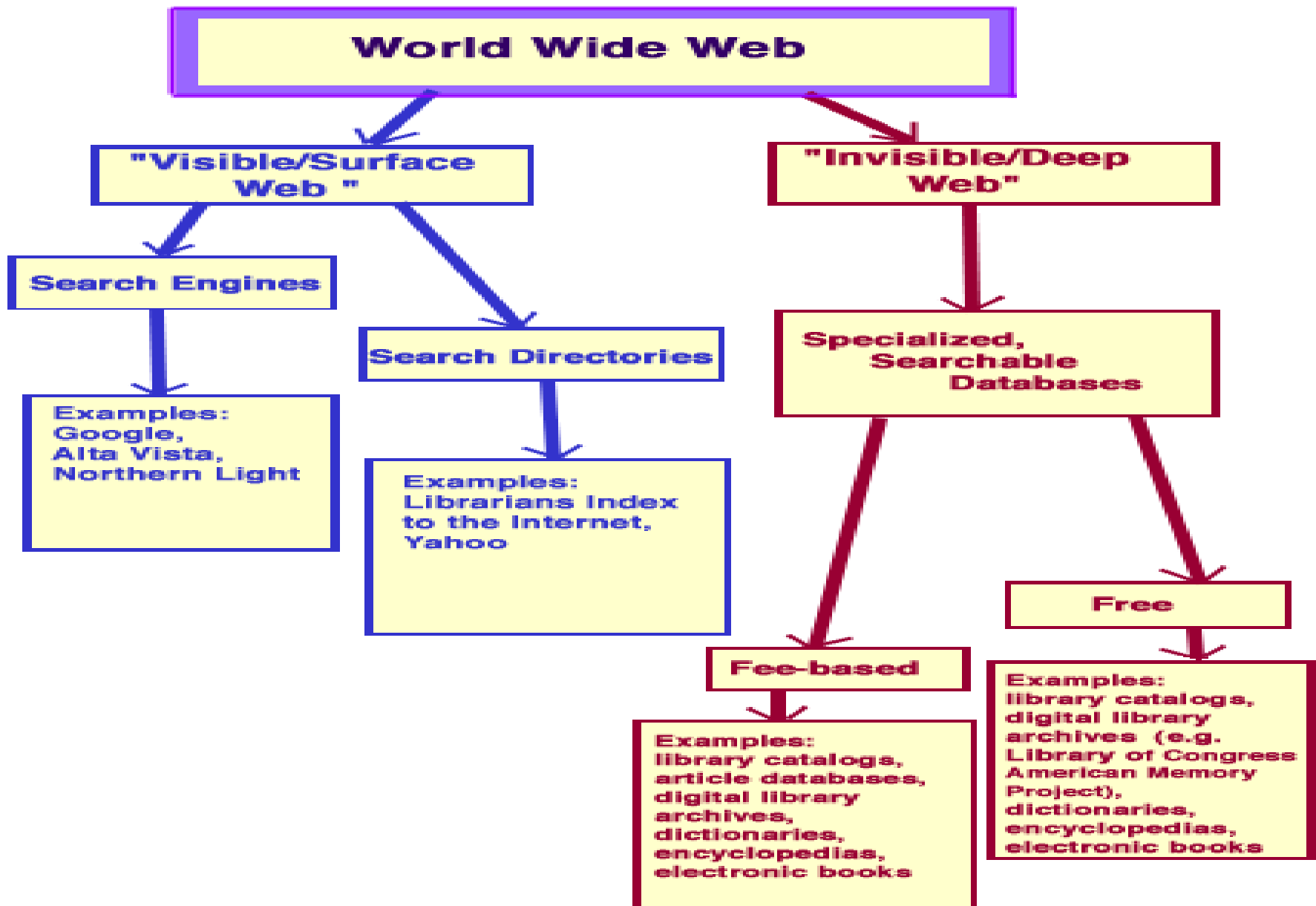
# BlockChain

- **Blockchain will emerge as the biggest challenge to the cyber law enforcement. India has yet to have cyber investigators and tools for this area.**



# The Internet, the Deep Web, and the Dark Web







# Indian Cyber Laws

Indian Cyber Laws were officially born on 17th October 2000 with the **Information Technology Act, 2000** coming into force.

- The **Indian Penal Code** (as amended by the IT Act) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.
- Digital Evidence is to be collected and proven in court as per the provisions of the **Indian Evidence Act** (as amended by the IT Act).
- In case of bank records, the provisions of the **Bankers' Book Evidence Act** (as amended by the IT Act) are relevant.
- Investigation and adjudication of cyber crimes is done in accordance with the provisions of **the Code of Criminal Procedure** and the IT Act.



# Self-incrimination

- **Self-incrimination** is the act of exposing oneself (generally, by making a statement) "to an accusation or charge of crime; to involve oneself or another [person] in a criminal prosecution or the danger thereof
- Self-incrimination can occur either directly or indirectly:
  - directly, by means of interrogation where information of a self-incriminatory nature is disclosed;
  - indirectly, when information of a self-incriminatory nature is disclosed voluntarily without pressure from another person.



# Right to Silence

- It is well established that the **Right to Silence** has been granted to the accused by virtue of the pronouncement in the case of **Nandini Sathpathy vs P.L.Dani**, no one can forcibly extract statements from the accused, who has the right to keep silent during the course of interrogation (investigation).
- By the administration of these tests, forcible intrusion into one's mind is being restored to, thereby nullifying the validity and legitimacy of the Right to Silence.



# Selvi & Ors vs State Of Karnataka & Anr on 5 May, 2010

- **“no individual should be forcibly subjected to any of the techniques in question, whether in the context of investigation in criminal cases or otherwise”. Doing so would amount to an unwarranted intrusion into personal liberty.**
- **However, any information or material that is subsequently discovered with the help of voluntary administered test results can be admitted, in accordance with Section 27 of the Evidence Act, 1872.**



# US Case Laws

- A ruling is explain the legal difference between a person's **identity and their knowledge**.
- “A communication is 'testimonial' only when it reveals the contents of your mind,”.
- “We can’t invoke the privilege against self-incrimination to prevent the government from collecting biometrics like fingerprints, DNA samples, or voice exemplars. Why?”
- Because the courts have decided that this evidence doesn’t reveal anything you know. It’s not testimonial.”



# US case Laws...

- ***U.S. v Doe* (11<sup>th</sup> Cir. 2012) 670 F.3d 1335**
- The Court concluded that decryption and production of the hard drives at issue “would require the use of the contents of Doe’s mind and could not be fairly characterized as a physical act that would be **non testimonial in nature.**”



# Evidentiary Value

- **Sec 4** of IT Act-2000. admissibility of e-records
- **Sec 65 B** of IEA..

any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed to be also a document



# Admissibility: Before Court

- **Evidence collection**
  - Correct legal processes
  - Accepted techniques and tools
  - Properly trained personnel
- **Chain of custody**
- **Testimony of Experts**
- **Corroboration**





# Admissibility of Electronic Evidence

- **65A and 65B** are introduced to the Evidence Act under the Second Schedule to the IT Act.
- **Section 5** of the Evidence Act provides that evidence can be given regarding only facts that are at issue or of relevance.
- **Section 136** empowers a judge to decide on the admissibility of the evidence. Section 65A provides that the contents of electronic records may be proved in accordance with the provisions of Section 65B.
- **Section 65B** provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic record (ie, the contents of a document or communication printed on paper that has been stored, recorded and copied in optical or magnetic media produced by a computer ('computer output')), is deemed to be a document and is admissible in evidence without further proof of the original's production, provided that the conditions set out in Section 65B(2) to (5) are satisfied.



# Admissibility: In Court

- **Presentation techniques**
  - Graphics – “Showing and telling is better than just telling”
  - Ask them to explain the story if the technical issues are complex
- Made it as simple as by using appropriate techniques
- Dr. Prakash case



# 1. State of Maharashtra vs. Dr. Praful B Desai (AIR 2003 SC 2053)

- [The question involved whether a witness can be examined by means of a video conference.]
- The Supreme Court observed that video conferencing is an advancement of science and technology which permits seeing, hearing, and talking with someone who is not physically present with the same facility and ease as if they were physically present.



## 2. Bodala Murali Krishna vs. Smt. Bodala Prathima (2007 (2) ALD 72)

- The court held that, “...the amendments carried to the Evidence Act by introduction of Sections 65-A and 65-B are in relation to the electronic record. Sections 67-A and 73-A were introduced as regards proof and verification of digital signatures.



# 3. Dharambir vs. Central Bureau of Investigation (148 (2008) DLT 289)

- The court arrived at the conclusion that when Section 65-B talks of an electronic record produced by a computer referred to as the computer output, it would also include a hard disc in which information was stored or was earlier stored or continues to be stored!



## 4. In Jagjit Singh vs. State of Haryana ((2006) 11 SCC 1)

- The speaker of the Legislative Assembly of the State of Haryana disqualified a member for defection. When hearing the matter, the Supreme Court considered the digital evidence in the form of interview transcripts from the Zee News television channel, the Aaj Tak television channel, and the Haryana News of Punjab Today television channel



# 5. Twentieth Century Fox Film Corporation vs. NRI Film Production Associates (P) Ltd. (AIR 2003 KANT 148)

- **In this case certain conditions have been laid down for video-recording of evidence:**
  - a) Before a witness is examined in terms of the Audio-Video Link, witness is to file an affidavit or an undertaking duly verified before a notary or a judge that the person who is shown as the witness is the same person as who is going to depose on the screen. A copy is to be made available to the other side. (Identification Affidavit).



# 6.State vs. Mohd. Afzal others

## HIGH COURT OF DELHI

- Terrorists had attacked the Parliament House on 13th December 2001.
- Digital evidence played an important role during their Trial.
- The Designated Judge of the Special Court constituted under (POTA) and Delhi HC during appeal had convicted/confirmed several accused persons.
- Later this judgment was overruled.





# 7. Anvar P.V. Vs P.K. Basheer and others ...

- **The Court has interpreted the Section 22A, 45A, 59, 65A & 65B of the Evidence Act and held that secondary data in CD/DVD/Pen Drive are not admissible without a certificate U/s 65 B(4) of Evidence Act. It has been elucidated that electronic evidence without certificate U/s 65B cannot be proved by oral evidence and also the opinion of the expert U/s 45A Evidence Act cannot be resorted to make such electronic evidence admissible.**



# 8.Sonu@Anvar Case vs State of Haryana

- **Sonu@Anvar** appeal in the Supreme Court, the argument was that the electronic document relied upon were not certified under Section 65B and hence were invalid technically. The appellant therefore sought that his conviction for abduction and murder should be set aside.
- **The Court decided that the appeal has to be rejected and in turn implied that at the appeal stage it is not necessary to re-open past cases where there has been no Section 65B certificate.**



# 9. Abdul Rahaman Kunji Vs. The State of West Bengal

- The Hon'ble High Court of Calcutta while deciding the admissibility of email held that an email downloaded and printed from the email account of the person can be proved by virtue of Section 65B r/w Section 88A of Evidence Act. The testimony of the witness to carry out such procedure to download and print the same is sufficient to prove the electronic communication



# 10. Jagdeo Singh Vs. The State and Ors.

- In the recent judgment pronounced by Hon'ble High Court of Delhi, while dealing with the admissibility of intercepted telephone call in a CD and CDR which were without a certificate u/s 65B Evidence Act, the court observed that the secondary electronic evidence without certificate u/s 65B Evidence Act is inadmissible and cannot be looked into by the court for any purpose whatsoever



# 11. Shreya Singhal v. Union of India

- Shreya Singhal v. Union of India is a judgement by a two-judge bench of the [Supreme Court of India](#) in 2015, on the issue of online speech and intermediary liability in India.
- The Supreme Court struck down Section 66A of the [Information Technology Act, 2000](#), relating to restrictions on online speech, unconstitutional on grounds of violating the freedom of speech guaranteed under Article 19(1)(a) of the [Constitution of India](#).
- The Court further held that the Section was not saved by virtue of being 'reasonable restrictions' on the freedom of speech under Article 19(2).
- The case was a watershed moment for online free speech in India.



# ***12.Dhariwal Industries Ltd. vs. Kishore Wadhvani & Ors.***

**Can a Complainant or Victim fight his own cyber crime case or appoint his own Lawyer?**

- It was held that Section 302 CrPC confers power on a magistrate to grant permission to the complainant to conduct the prosecution independently. The court also made it clear that the said provision applies to every stage, including the stage of framing charge

# Question Time

10 August 2017

# Contact me @....

- **919444049224**  
**drsmurugan.tnpol@gov.in**





Thank  
you

