Electronic Evidence: Collection, Preservation and Appreciation

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

Outline of My Presentation

- Cyber Crime
- EE: Acquisition, Authentication, Admissibility
- Chain of Custody : SOP, Hash value
- Social Media issues
- EE: 2020 Vision
- Recent Cybercrime trends
- Cyber Economics
- Tips for staying safe online
- Indian Cyber Laws
- Admissibility of EE : Case Laws.

Introduction

- **Technological revolution in communications and information technology. Impact of Social Media**

- **All Stake holders of judicial justice system need to update the use of latest technology and cyber forensic investigation techniques**

Edmond Locard (1877–1966)

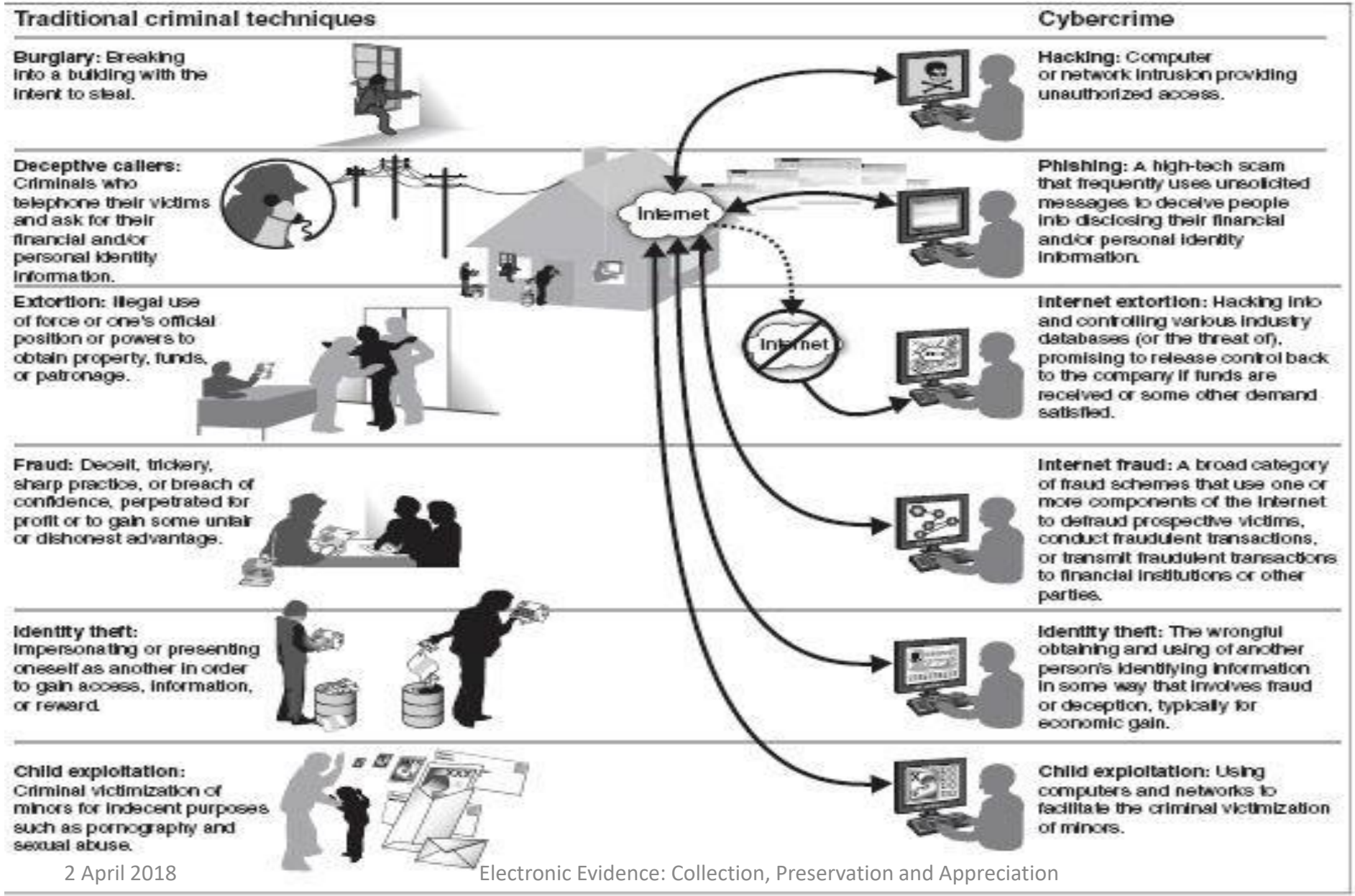
Locard's theory

" Anyone, or anything, entering a crime scene takes something of the crime scene with them. They also leave behind something of themselves when they depart"

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.
- Cybercriminals may use Information technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes.

Conventional Crimes Vs. Cyber Crimes



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: **Digital Evidence**
- **Binary Equivalent:**

01000100 01101001 01100111 01101001
01110100 01100001 01101100 00100000
01000101 01110110 01101001 01100100
01100101 01101110 01100011 01100101

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

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.
- Process of Acquisition, Authentication, and legal Admissibility of information stored on magnetic and or any other storage media is a challengeable task in Electronic evidence.
- Cyber forensics is the application of science and engineering to the legal problem of Electronic evidence. It is a synthesis of science and law.

Electronic Evidence plays larger role in Criminal Investigations

- **Evidence from ECD continues to play a larger role in the search for justice.“To try to show “**
- **What was happened ?**

How it was happened ?

When it was happened?

Challenges with Electronic Evidence

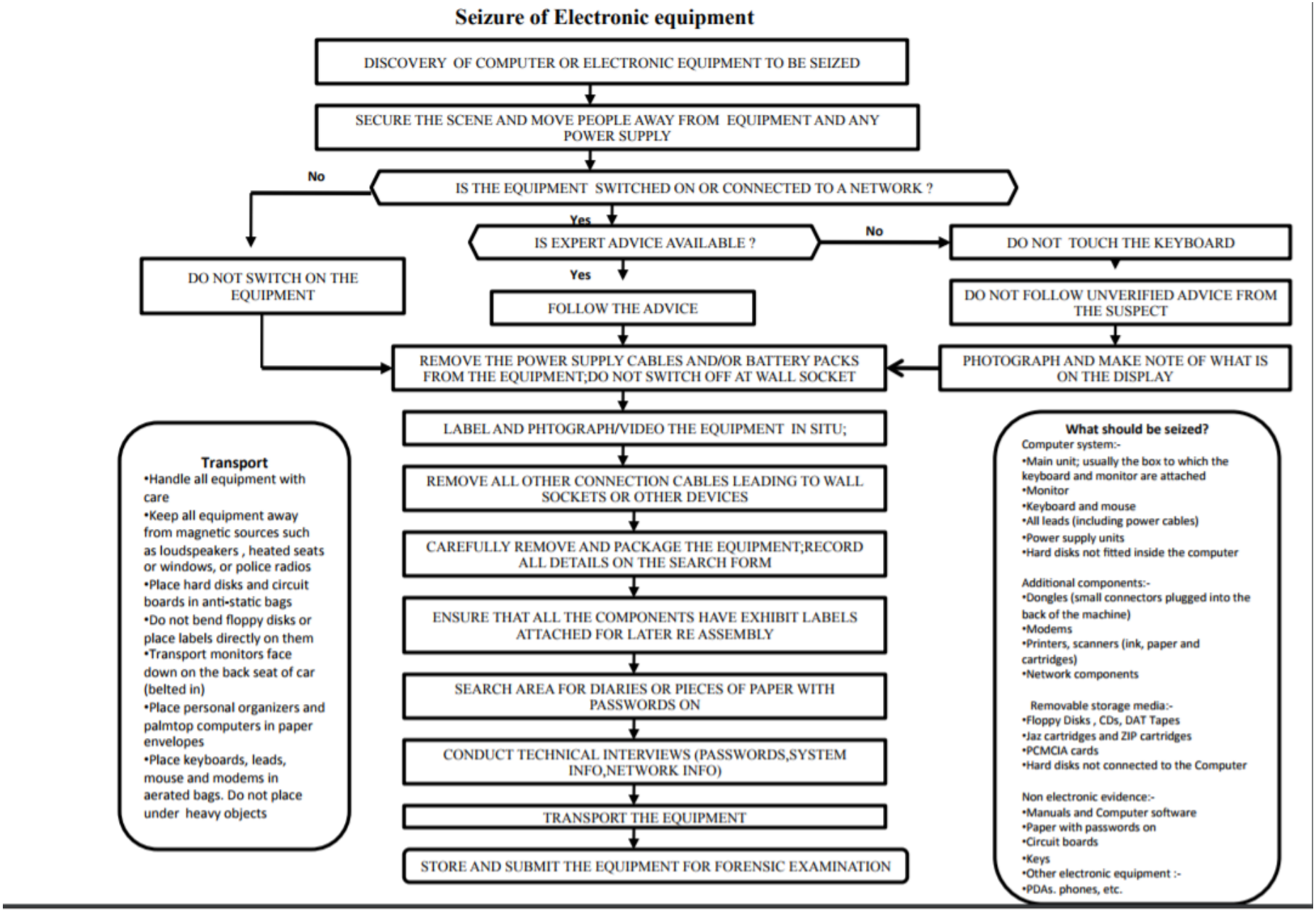
- **Electronic evidence, by its very nature is invisible to the eye, must be developed using tools other than the human eye.**
- **Each step requires the use of specialised tools or/and knowledge, the process must be documented, reliable and repeatable.**
- **The process itself must be understandable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

Challenges with Electronic Evidence

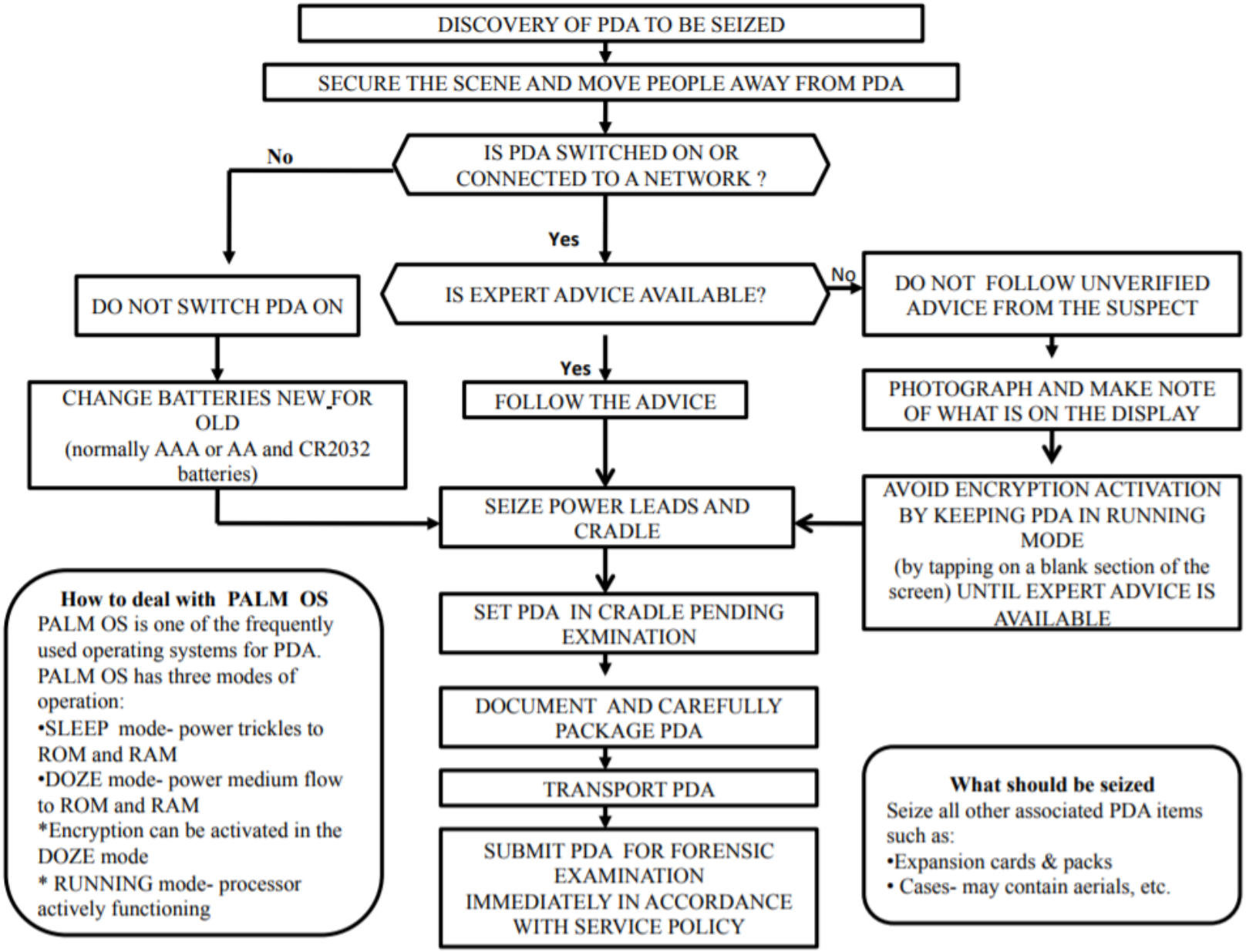
- **Acquisition of evidence is both a legal and technical problem.**
- **The law specifies what can be seized, under what conditions, from whom, and from where it may be seized. The determination of what a particular piece of digital evidence is, requires its examination.**

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;"***


Seizure of Electronic equipment
DISCOVERY OF COMPUTER OR ELECTRONIC EQUIPMENT TO BE SEIZED
SECURE THE SCENE AND MOVE PEOPLE AWAY FROM EQUIPMENT AND ANY POWER SUPPLY
IS THE EQUIPMENT SWITCHED ON OR CONNECTED TO A NETWORK ?
No
Yes
DO NOT SWITCH ON THE EQUIPMENT
IS EXPERT ADVICE AVAILABLE ?
No
Yes
DO NOT TOUCH THE KEYBOARD
FOLLOW THE ADVICE
DO NOT FOLLOW UNVERIFIED ADVICE FROM THE SUSPECT
REMOVE THE POWER SUPPLY CABLES AND/OR BATTERY PACKS FROM THE EQUIPMENT;DO NOT SWITCH OFF AT WALL SOCKET
PHOTOGRAPH AND MAKE NOTE OF WHAT IS ON THE DISPLAY
LABEL AND PHTOGRAPH/VIDEO THE EQUIPMENT IN SITU;
REMOVE ALL OTHER CONNECTION CABLES LEADING TO WALL SOCKETS OR OTHER DEVICES
CAREFULLY REMOVE AND PACKAGE THE EQUIPMENT;RECORD ALL DETAILS ON THE SEARCH FORM
ENSURE THAT ALL THE COMPONENTS HAVE EXHIBIT LABELS ATTACHED FOR LATER RE ASSEMBLY
SEARCH AREA FOR DIARIES OR PIECES OF PAPER WITH PASSWORDS ON
CONDUCT TECHNICAL INTERVIEWS (PASSWORDS,SYSTEM INFO,NETWORK INFO)
TRANSPORT THE EQUIPMENT
STORE AND SUBMIT THE EQUIPMENT FOR FORENSIC EXAMINATION
Transport
•Handle all equipment with care
•Keep all equipment away from magnetic sources such as loudspeakers , heated seats or windows, or police radios
•Place hard disks and circuit boards in anti-static bags
•Do not bend floppy disks or place labels directly on them
•Transport monitors face down on the back seat of car (belted in)
•Place personal organizers and palmtop computers in paper envelopes
•Place keyboards, leads, mouse and modems in aerated bags. Do not place under heavy objects
What should be seized?
Computer system:-
•Main unit; usually the box to which the keyboard and monitor are attached
•Monitor
•Keyboard and mouse
•All leads (including power cables)
•Power supply units
•Hard disks not fitted inside the computer
Additional components:-
•Dongles (small connectors plugged into the back of the machine)
•Modems
•Printers, scanners (ink, paper and cartridges)
•Network components
Removable storage media:-
•Floppy Disks , CDs, DAT Tapes
•Jaz cartridges and ZIP cartridges
•PCMCIA cards
•Hard disks not connected to the Computer
Non electronic evidence:-
•Manuals and Computer software
•Paper with passwords on
•Circuit boards
•Keys
•Other electronic equipment :-
•PDAs. phones, etc.

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 it’s 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

Types of Digital Forensics

- 1.Computer Forensics.
- 2. Network Forensics.
- 3.Mobile device Forensics.
- 4. IoT Forensics.
- 5. Cloud Forensics
- 6. Voice Forensics
- 7.Photo Forensics

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.

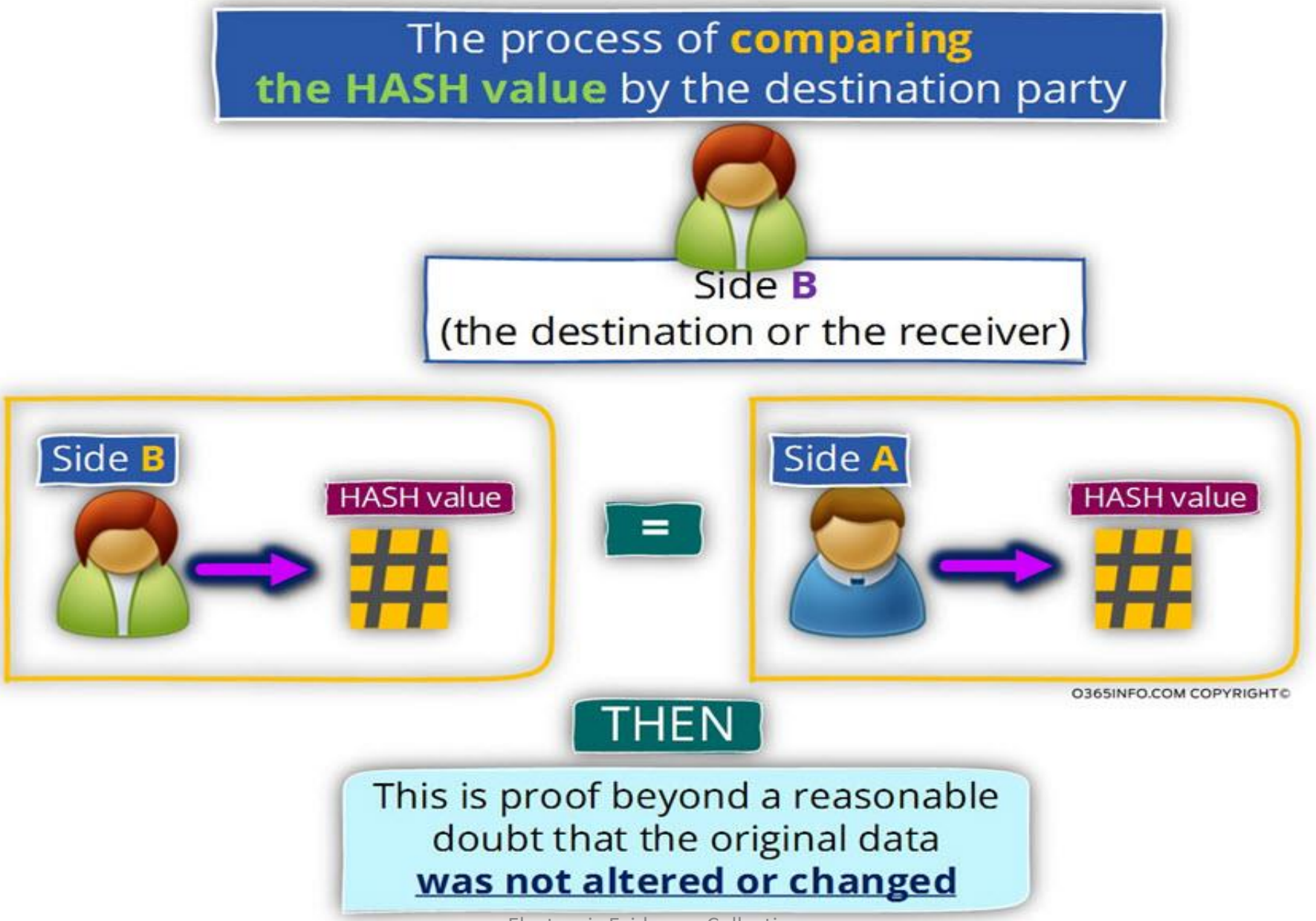
Wiping a file

- **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

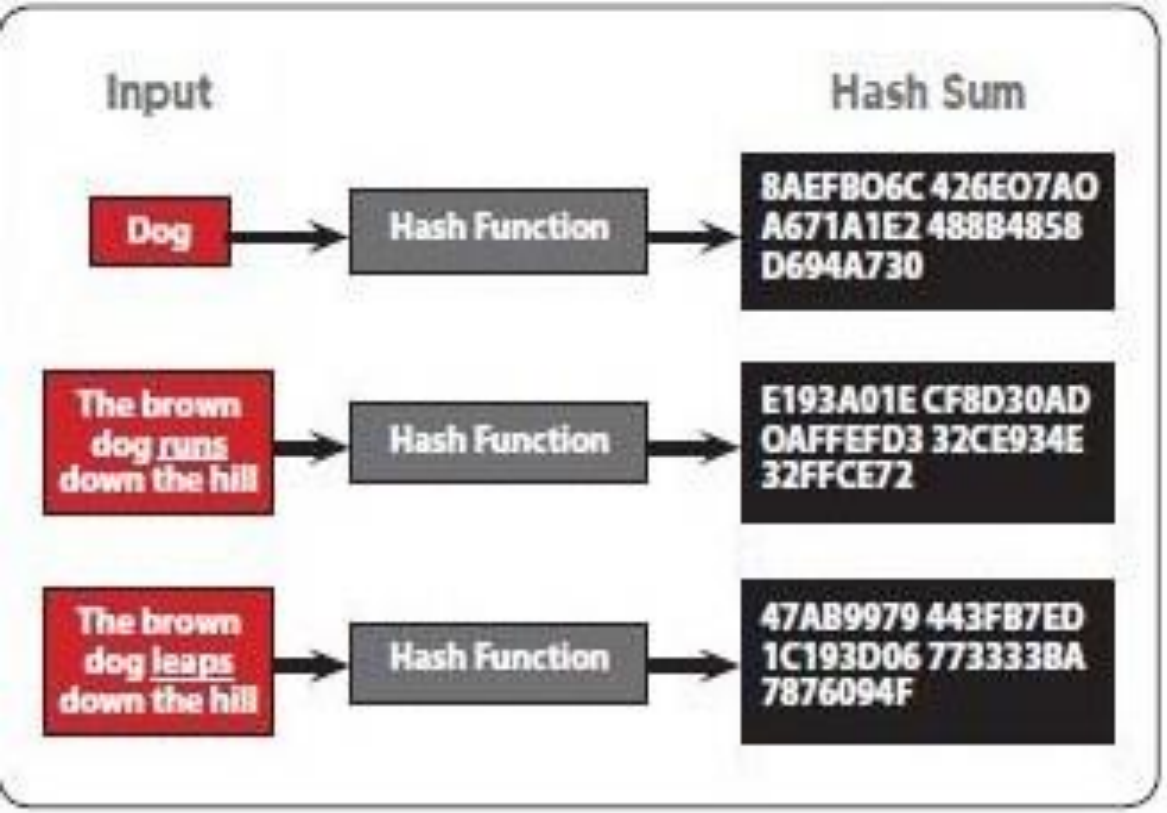
Hash value

- 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


The process of comparing the HASH value by the destination party
Side B
(the destination or the receiver)
Side B
HASH value
=
Side A
HASH value
O365INFO.COM COPYRIGHT©
THEN
This is proof beyond a reasonable doubt that the original data was not altered or changed

How Are Evidence Copies Verified?

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



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…
- Many 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, 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 IPC , 354A, 354B, 354C and 354D IPC
- 4. Netizen Rights
- Ban on Social Media
- Sec 144 Crpc
- Sec 5 of ITA 1885

SCI upholds Internet ban by States

- **SCI 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,**
- **Patidar agitation led by Hardik Patel**
- **Section 144 of the CrPC.**

  Gaurav Sureshbhai Vas Vs State of Gujarat 2016

  "It becomes very necessary sometimes for law and order," CJI Thakur observed while dismissing his appeal.

  Similar bans have been imposed in other states, including Jammu & Kashmir, whenever the police has apprehended a law and order problem.

Germany's €50m fines for social media companies

- **German enacted a law in favour of fines of up to €50m for social media companies that regularly fail to swiftly remove illegal content from their platforms.**
- **The new law comes into force in October 2017 and compels firms such as Twitter, YouTube and Facebook to take down obviously criminal material within 24 hours and to assess content that is not clearly unlawful within seven days.**

Free wifi

- All the Airports are connected with free wifi for an hour at lest to all by service providers
- Google has installed free wifis 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.
- Netflow analysis will show them all we have on our cellphones, what VPN service we use, what customized projects we have..etc
- Master surveillance plan

Are you safe with your e mail Accounts?

Gmail,yahoo,etc not safe

No social media platform is safe

.ios/ icloud also not safe!

Use privacy settings pl

Use your own e mail accounts..

Driver behaviour service

IBM Watson IoT Driver Behaviour Service lets you analyze drivers' behavior from vehicle probe data and contextual data

You can analyze driver behavior such as harsh acceleration and harsh braking, frequent braking, speeding, sharp turn, and so on.

Useful for Accident/ Insurance cases investigations!

EE: 2020 Vision…

- **Software will disrupt most traditional industries in the next 5-10 years.**
  - **Uber**
  - **Airbnb**
  - **IBM Watson,**
- **Autonomous cars:**
- **In 2018 the first self driving cars**
- **Around 2020, the complete Automobile industry will start to be disrupted.**
- **You don't want to own a car anymore.**
- **Next generation will never get a driving license and will never own a car.**

Autonomous cars:

- In 2018 the first self driving cars
- Around 2020, the complete Automobile industry will start to be disrupted.
- You don't want to own a car anymore.
- Just a phone call
- Next generation will never get a drivering license and will never own a car.

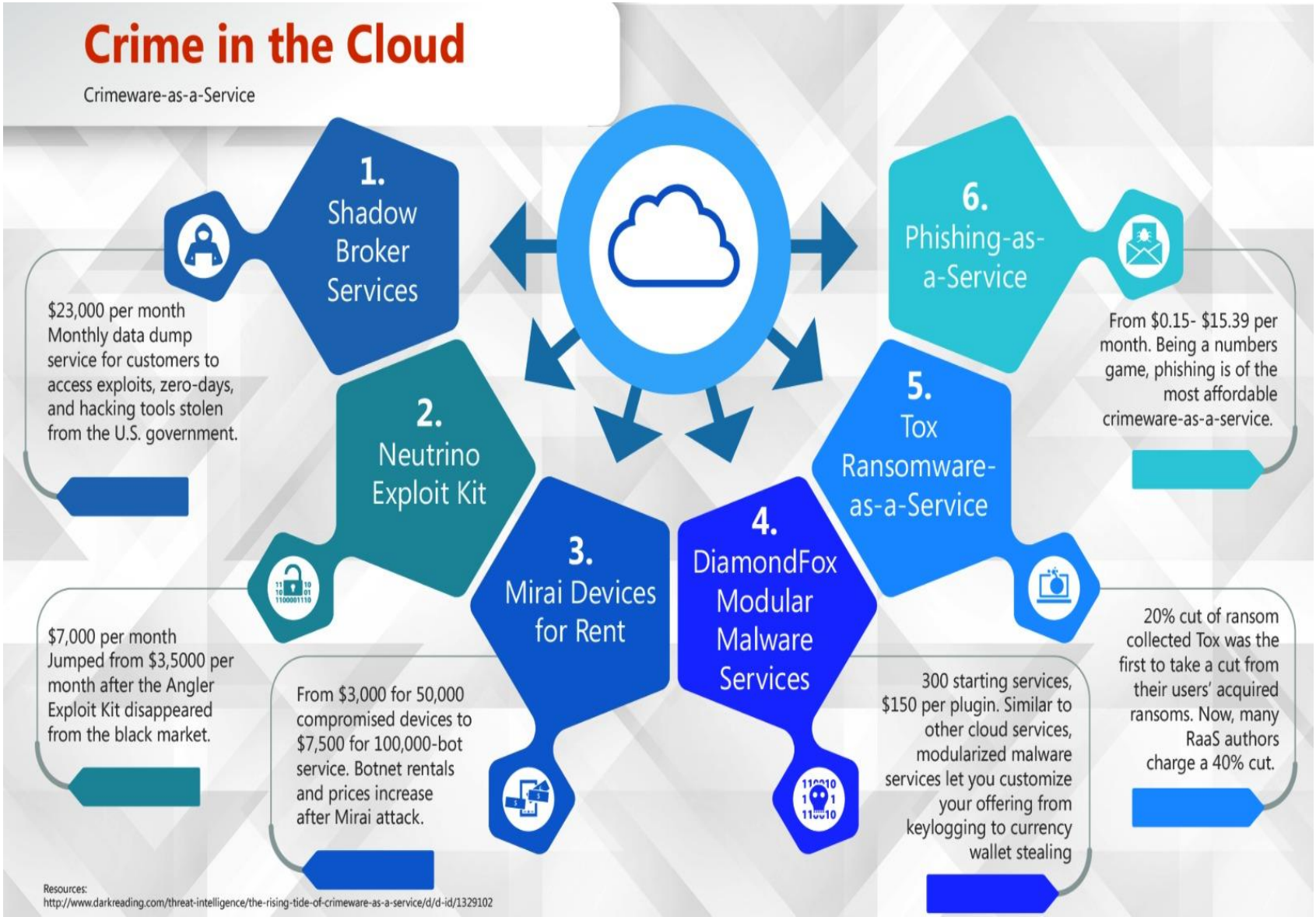
Zero Accident, no car parking…

- No need for huge Car Parking
- we can save a million lives each year.
- Insurance companies
- Real estate will change.
- Medical tourism

Recent cybercrime trends

1: Crime-as-a-Service

The digital underground is underpinned by a growing Crime-as-a-Service model that interconnects specialist providers of cybercrime tools and services with an increasing number of organised crime groups. Terrorist actors clearly have the potential to access this sector in the future.


Crime in the Cloud
Crimeware-as-a-Service
1. Shadow Broker Services
$23,000 per month
Monthly data dump service for customers to access exploits, zero-days, and hacking tools stolen from the U.S. government.
2. Neutrino Exploit Kit
$7,000 per month
Jumped from $3,5000 per month after the Angler Exploit Kit disappeared from the black market.
3. Mirai Devices for Rent
From $3,000 for 50,000 compromised devices to $7,500 for 100,000-bot service. Botnet rentals and prices increase after Mirai attack.
4. DiamondFox Modular Malware Services
300 starting services, $150 per plugin. Similar to other cloud services, modularized malware services let you customize your offering from keylogging to currency wallet stealing
5. Tox Ransomware-as-a-Service
20% cut of ransom collected Tox was the first to take a cut from their users' acquired ransoms. Now, many RaaS authors charge a 40% cut.
6. Phishing-as-a-Service
From $0.15- $15.39 per month. Being a numbers game, phishing is of the most affordable crimeware-as-a-service.
Resources:
http://www.darkreading.com/threat-intelligence/the-rising-tide-of-crimeware-as-a-service/d/d-id/1329102

2.Ransomware

Ransomware

Ransomware and banking Trojans remain the top malware threats, a trend unlikely to change for the foreseeable future.

3.The criminal use of data

Aadhar Data leaking

Apple , Facebook, Samsung

Biometric data Finger print eye scan

4: Payment fraud

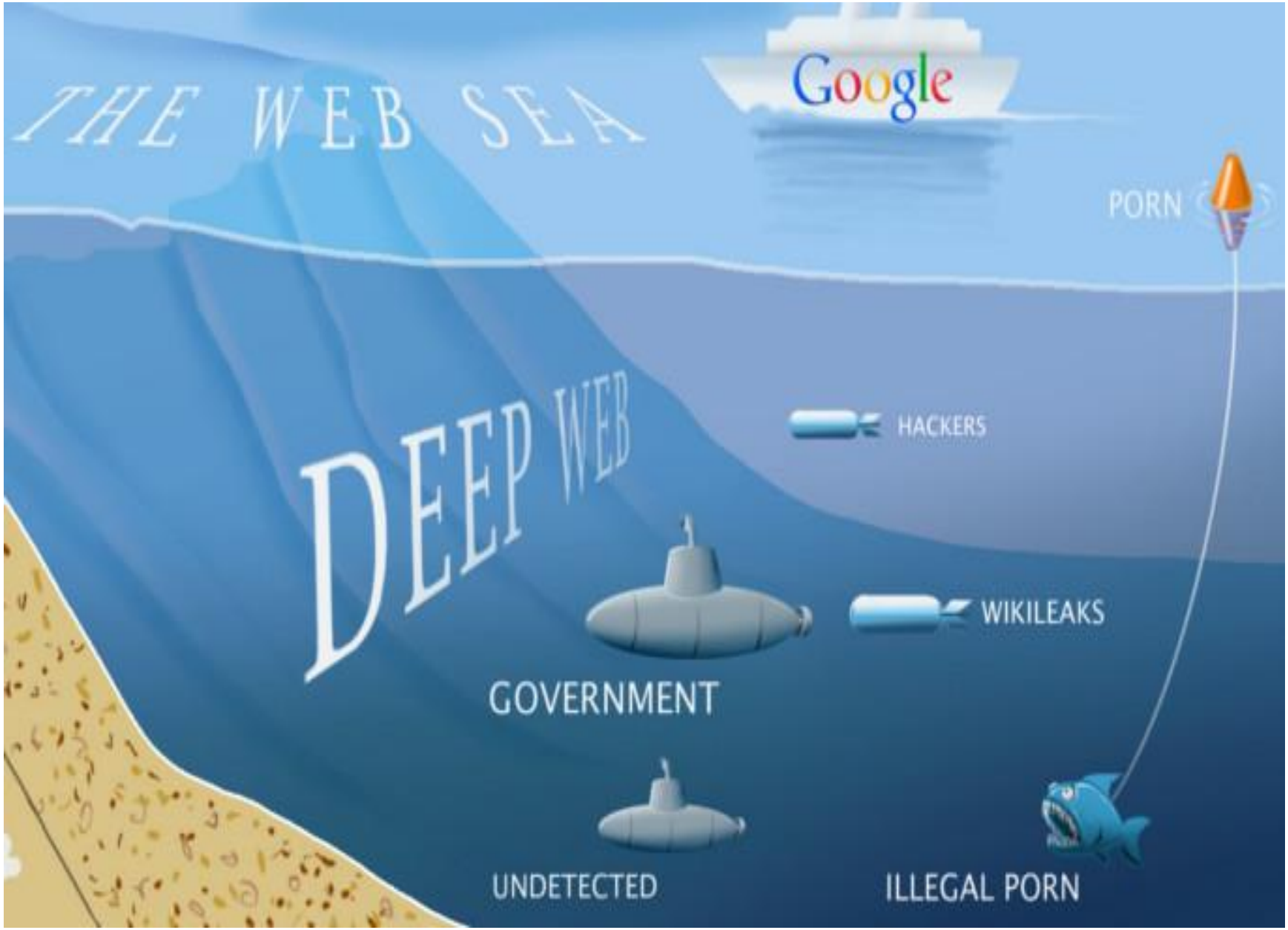
All type of on line off line frauds

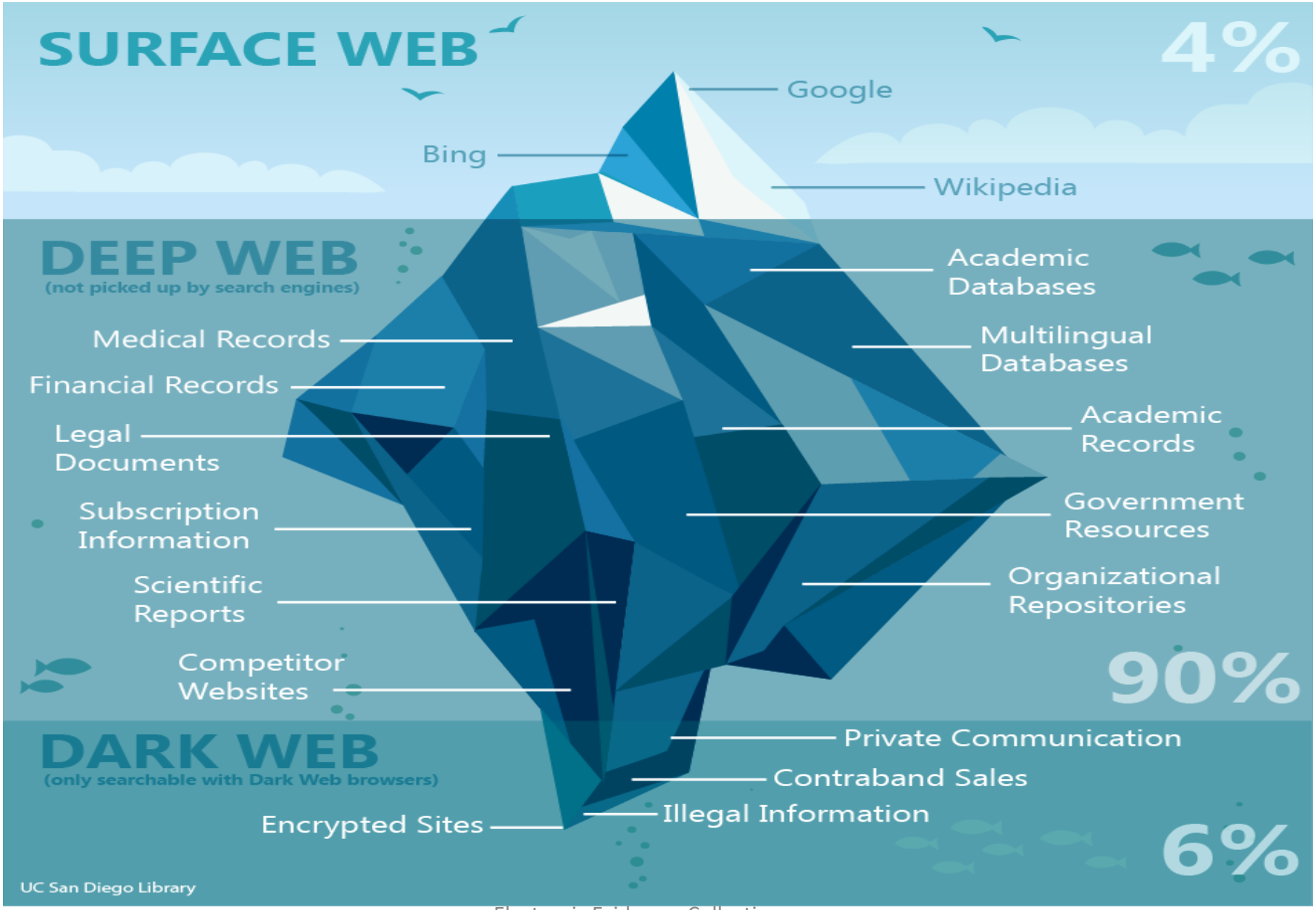
ATM frauds

5: Online child sexual abuse

Pornography

Child pornography


THE WEB SEA
Google
PORN
DEEP WEB
HACKERS
WIKILEAKS
GOVERNMENT
UNDETECTED
ILLEGAL PORN


SURFACE WEB
4%
Google
Bing
Wikipedia
DEEP WEB
(not picked up by search engines)
Academic Databases
Medical Records
Multilingual Databases
Financial Records
Academic Records
Legal Documents
Government Resources
Subscription Information
Organizational Repositories
Scientific Reports
Competitor Websites
90%
DARK WEB
(only searchable with Dark Web browsers)
Private Communication
Contraband Sales
Illegal Information
Encrypted Sites
6%
UC San Diego Library

6.Deep web challenges

- 1.Accessing the Dark Web
- Accessing the dark web is to download "TOR" The Onion Router Browser Bundle" from TorProject.org.
- 2.Anonymously and illegal
- 3.invisible web
- 4.Silk Road1.0 (Oct 2013)
- Silk Road2.0 (Nov 2014)
- Silk Road3.0 (May 2017)
- 5. Untraceable crypto currencies

7: Social engineering

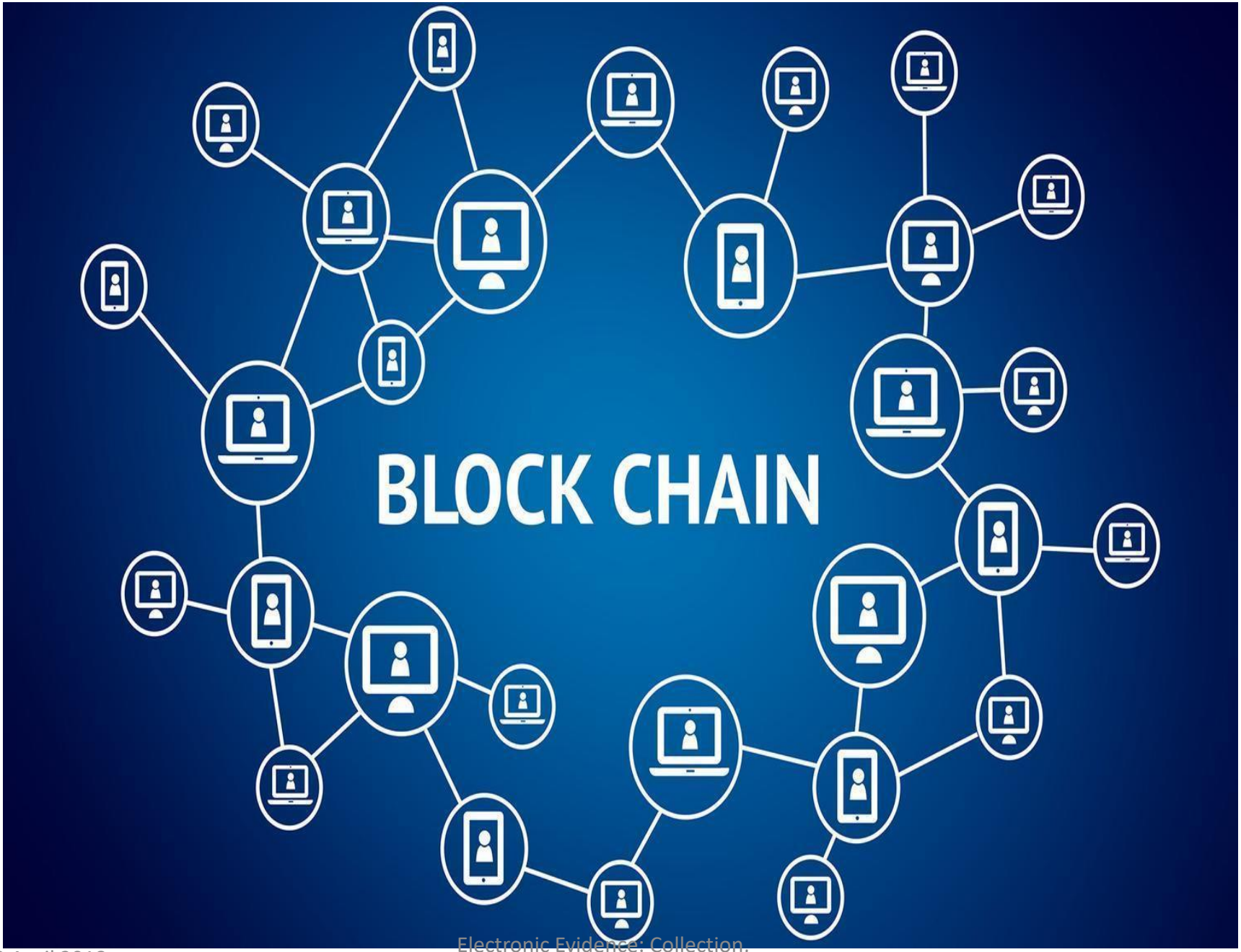
An increase of phishing aimed at high value targets has been registered by enforcement private sector authorities.

8: Virtual currencies

Bitcoin remains the currency of choice for the payment for criminal products and services in the digital underground economy and the Darknet. Bitcoin has also become the standard payment solution for extortion payments

Block chain

- **The blockchain is an undeniably ingenious invention – the brainchild of a person or group of people known by the Satoshi Nakamoto.**
- **The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value**


BLOCK CHAIN

Blockchain Application

- Digital Identities
- Health
- Distributed cloud Storage
- Digital Voting

  Passports
- E-Residency
- Birth /death Certificates
- Wedding Certificates
- Land Records
- Online Account Login

2017: high-profile data breaches

Yahoo data breach actually hit three billion accounts

Almost all yahoo mail accounts were compromised!

Deloitte

Global consultancy firm Deloitte has been compromised through an unsecured administrator account, which allowed access to internal files. Details compromised include emails, usernames, passwords, health information, and details from Deloitte's clients.

Equifax

Consumer credit score company Equifax has revealed that hackers accessed up to 143 million customer account details taken include names, social security numbers, drivers licences, and credit card numbers of around 200,000 pec

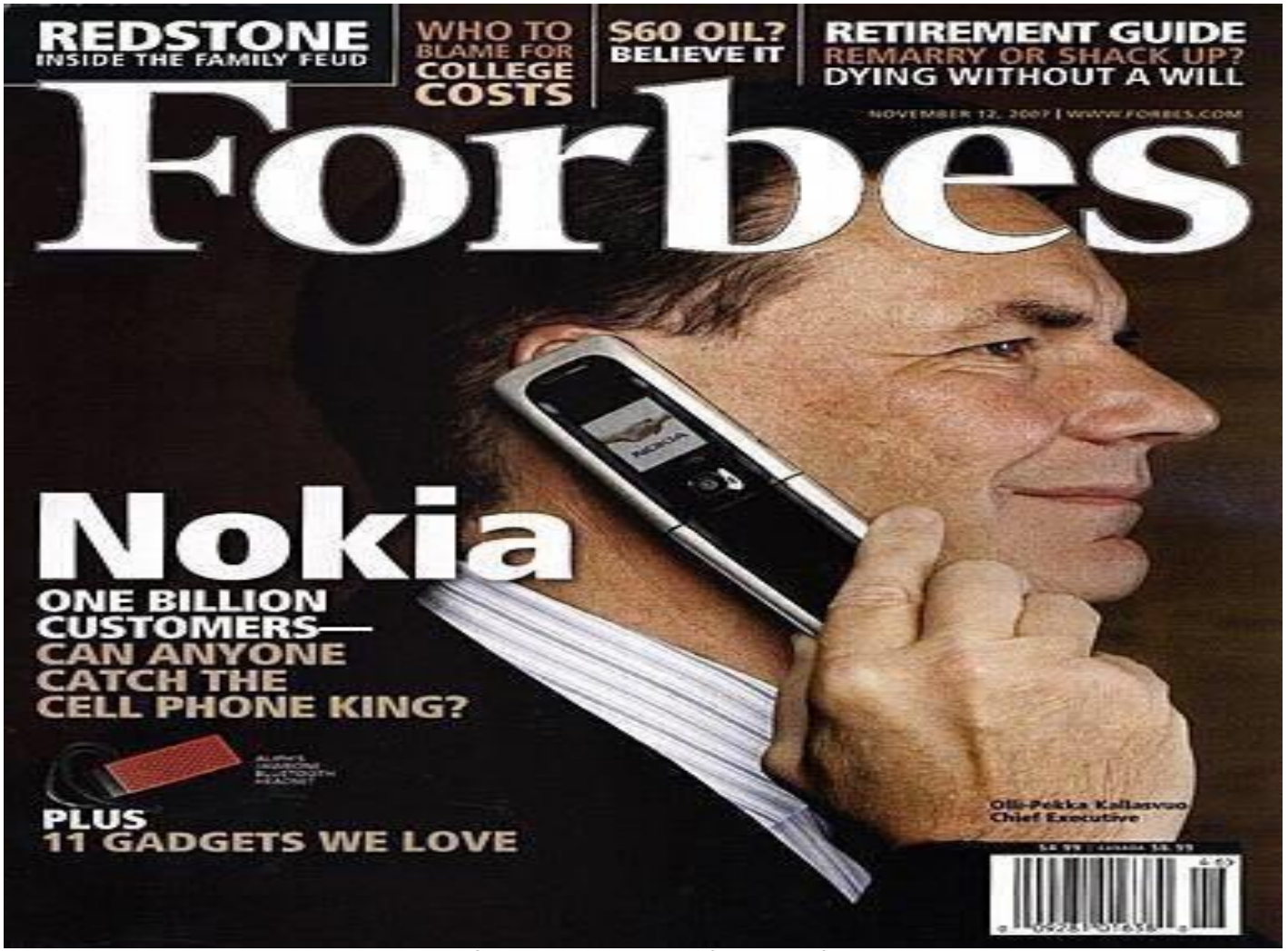
Verizon

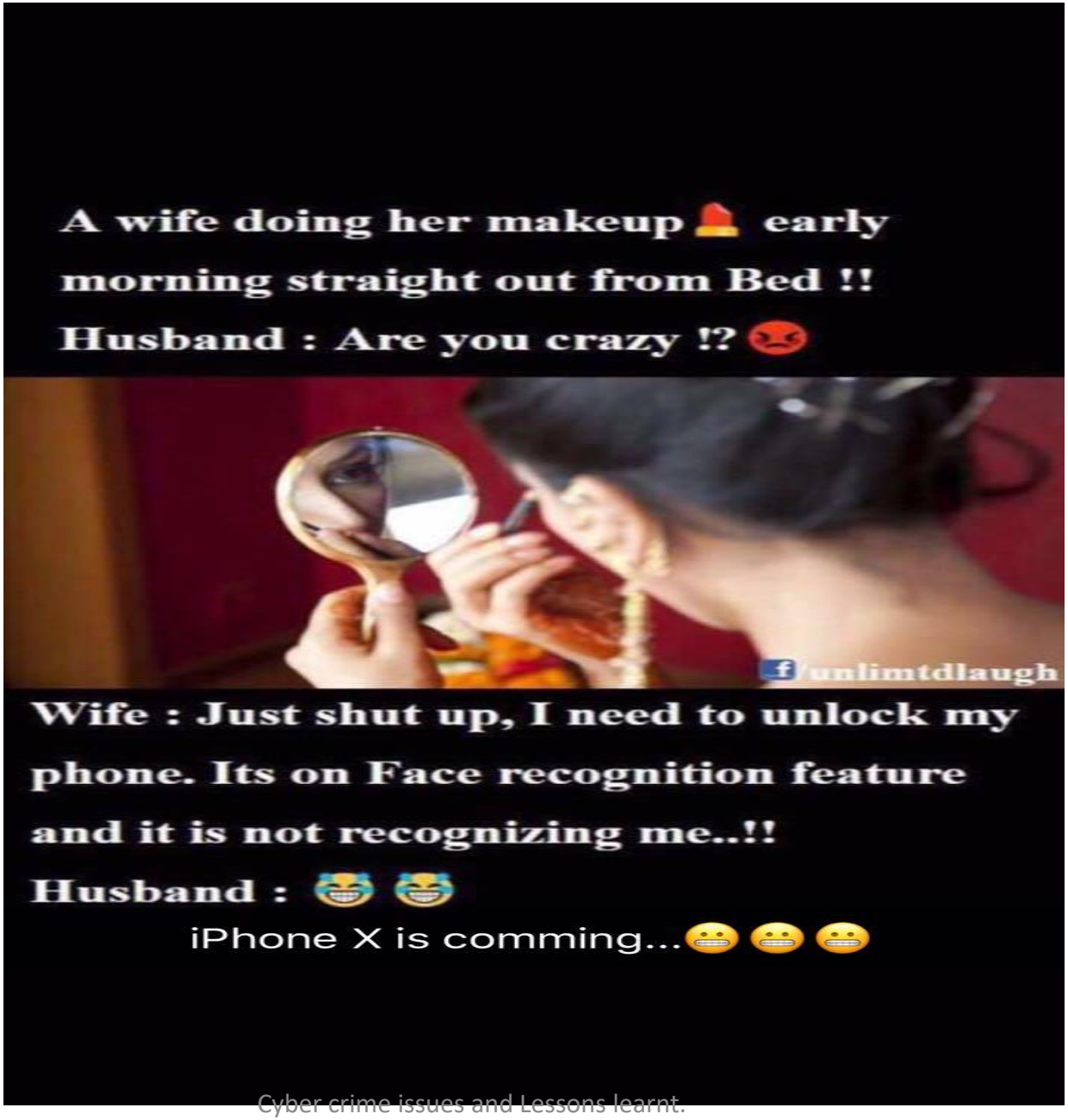
Phone numbers, names and pin codes of of six million Verizon customers were left online for around nine days. A misconfigured setting on a cloud server led to the details being posted online

Uber : cyber attack that exposed 57 million people's data

- **Hackers stole the personal data of 57 million customers and drivers from Uber, a massive breach that the company concealed for more than a year.**

10 years ago....Forbes, cover story...and we all know, what eventually happened.....




A wife doing her makeup early morning straight out from Bed !!
Husband : Are you crazy !?
unlimtdlaugh
Wife : Just shut up, I need to unlock my phone. Its on Face recognition feature and it is not recognizing me..!!
Husband :
iPhone X is comming...

No Technology is Secure forever, its just Secure for that instance of time"

- iPhone X series onwards Apple has introduced 'Facial Recognition' Tech to unlock phone and access data on its smartphones,
- previously apple used Biometric Fingerprint to unlock phones.
- Hackers have found a way to circumvent even latest facial recognition technology faking actual user using 3D Printed Masks so even the most expensive iPhone gets unlocked.
- "**No Technology is Secure forever, its just Secure for that instance of time"**

FBI vs Apple

- **2015 mass shootings in San Bernadino, California.**
- **Two shooters (couple)were involved, who murdered 14 people before fleeing from the police a rented vehicle, only to end up dead themselves after trying to shoot it out with the police from inside their car.**
- **The couple had apparently destroyed their own mobile phones before undertaking the attack, but the husbands's work phone, technically the property of the San Bernadino council, was bagged by the FBI to see what investigative intelligence it could reveal, if any.**
- **That's what led to the court case, when the FBI found itself stuck up against the iPhone's passcode.**

CyberEconomics :

- 'Amazon Pantry' - Delivers Grocery by NextDay in few Cities including Chennai
- Interestingly there were no GST, shipping charges laid, Rebate on MRP - *discounts absorbed* taxes too.
- Paytm is the tremendous example of Explosive e-Commerce growth.
- Big basket, Just buy

Business Model ?

- Last year Amazon declared its losses to
- $ 100 Million, Grabbing more UserBase is the whole agenda .
- whatsapp bagged 1900 Crore Investment with 50 employees for 45 Crore UsersBase in 2014.
- Jio launched Revolutionary Technology of VOLTE which offered free 4G calling , Jio is set to absorb 19,600 Crore Losses in FY17-FY18, till considerable userbase is formed, it persists to carry on awaiting for the Return of Investment (ROI) projected to be recovered by 2022.
- Snap deal !

IoT devices becoming 'cyberweapon of choice' for attackers

- **North Korea Model**

Wannacry

Remote Neural Monitoring: How They Spy on Your Thoughts

- **National Security Agency (NSA) of the U.S.A. has developed a very efficient method of controlling the human brain.** This technology is called ***Remote Neural Monitoring (R.N.M.)*** and is expected to revolutionize crime detection and investigation.

- **R.N.M. works remotely** (ever wondered why have we all been driven relentlessly towards wireless systems?) **to control the brain under the objective to detect any criminal thought taking place inside the mind of a possible culprit.** Inevitable question: How can you isolate a criminal thought if you do not have a comparative measure of non-criminal thoughts.

'Fintech'

- **Fintech is a portmanteau of financial technology that describes an emerging financial services sector in the 21st century.**
- **Originally, the term applied to technology applied to the back-end of established consumer and trade financial institutions.**
- **Since the end of the first decade of the 21st century, the term has expanded to include any technological innovation in the financial sector, including innovations in financial literacy and education, retail banking, investment and even crypto-currencies like bitcoin.**

New Tech in Fintech

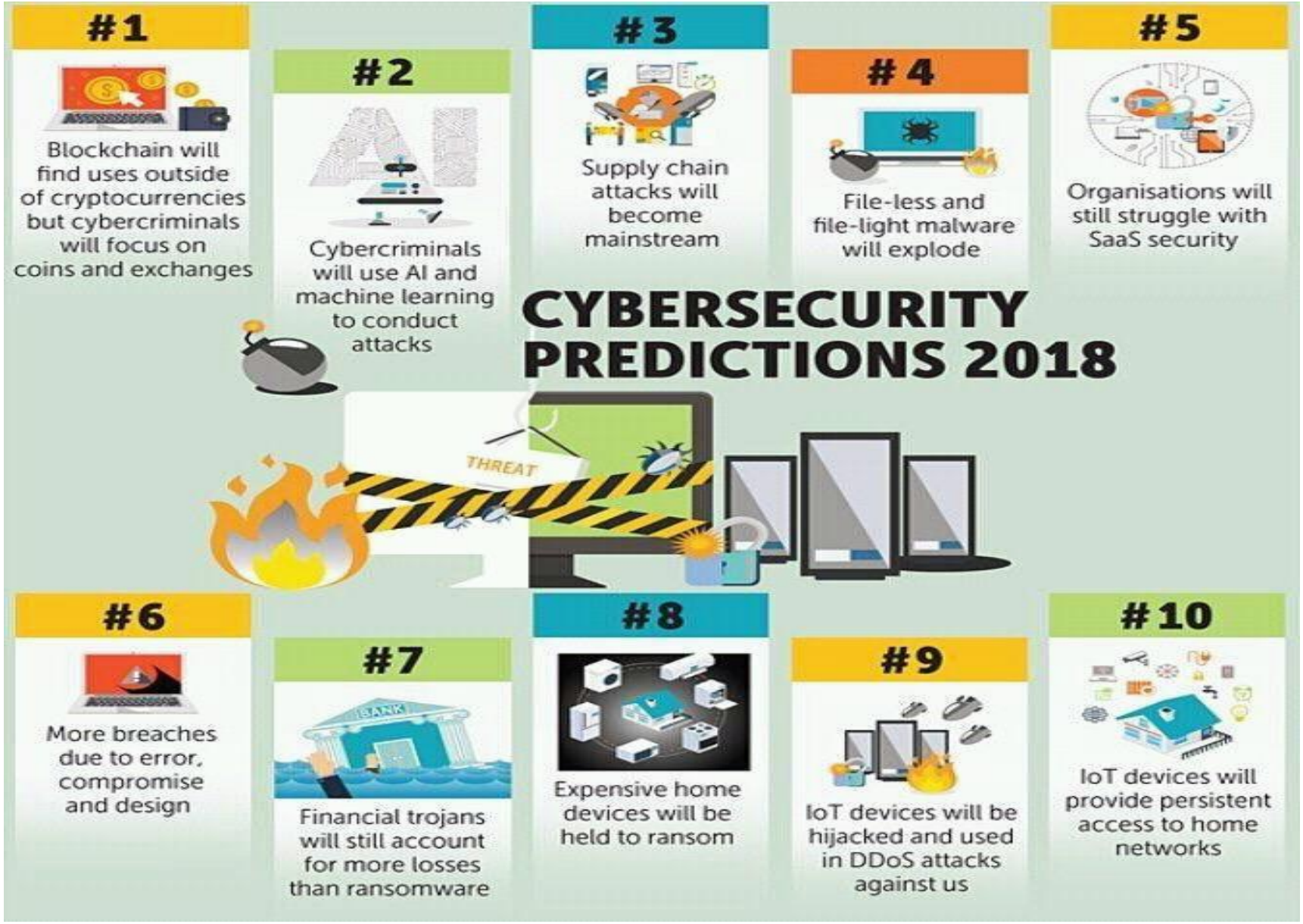
- New technologies, like machine learning/artificial intelligence, predictive behavioral analytics and data-driven marketing, will take the guesswork and habit out of financial decisions. "Learning" apps will not only learn the habits of users, often hidden to themselves, but will engage users in learning games to make their automatic, unconscious spending and saving decisions better

Fintech innovation avenues

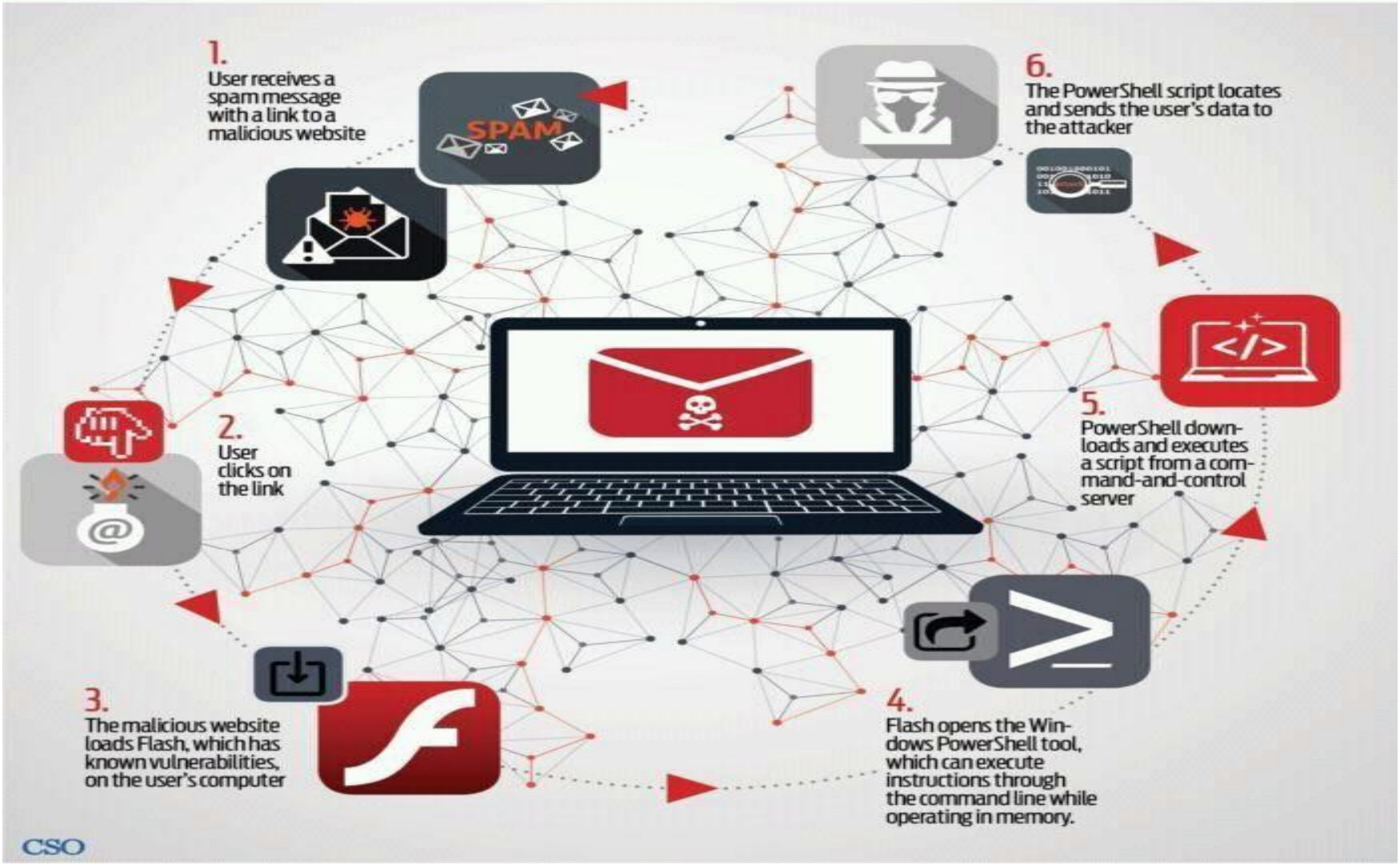
- Cryptocurrency and digital cash Blockchain technology, including Etherium, a distributed ledger technology (DLT) that maintain records on a network of computers, but has no central ledger.
- Smart contracts, which utilize computer programs (often utilizing the blockchain) to automatically execute contracts between buyers and sellers.
- Open banking, a concept that leans on the blockchain and posits that third-parties should have access to bank data to build applications that create a connected network of financial institutions and third-party providers. An example is the all-in-one money management tool Mint

Fintech innovation avenues…

- Insurtech, which seeks to use technology to simplify and streamline the insurance industry.
- Regtech, which seeks to help financial service firms meet industry compliance rules, especially those covering Anti-Money Laundering and Know Your Customer protocols which fight fraud.
- Robo-advisors, such as Betterment, utilize algorithms to automate investment advice to lower its cost and increase accessibility.
- Unbanked/underbanked, services that seek to serve disadvantaged or low-income individuals who are ignored or underserved by traditional banks or mainstream financial services companies.
- Cybersecurity, given the proliferation of cybercrime and the decentralized storage of data, cybersecurity and fintech are interlocked.


#1
Blockchain will find uses outside of cryptocurrencies but cybercriminals will focus on coins and exchanges
#2
AI
Cybercriminals will use AI and machine learning to conduct attacks
#3
Supply chain attacks will become mainstream
#4
File-less and file-light malware will explode
#5
Organisations will still struggle with SaaS security
CYBERSECURITY PREDICTIONS 2018
THREAT
#6
More breaches due to error, compromise and design
#7
BANK
Financial trojans will still account for more losses than ransomware
#8
Expensive home devices will be held to ransom
#9
IoT devices will be hijacked and used in DDoS attacks against us
#10
IoT devices will provide persistent access to home networks

How a **FILELESS ATTACK** works



Tips for staying safe online

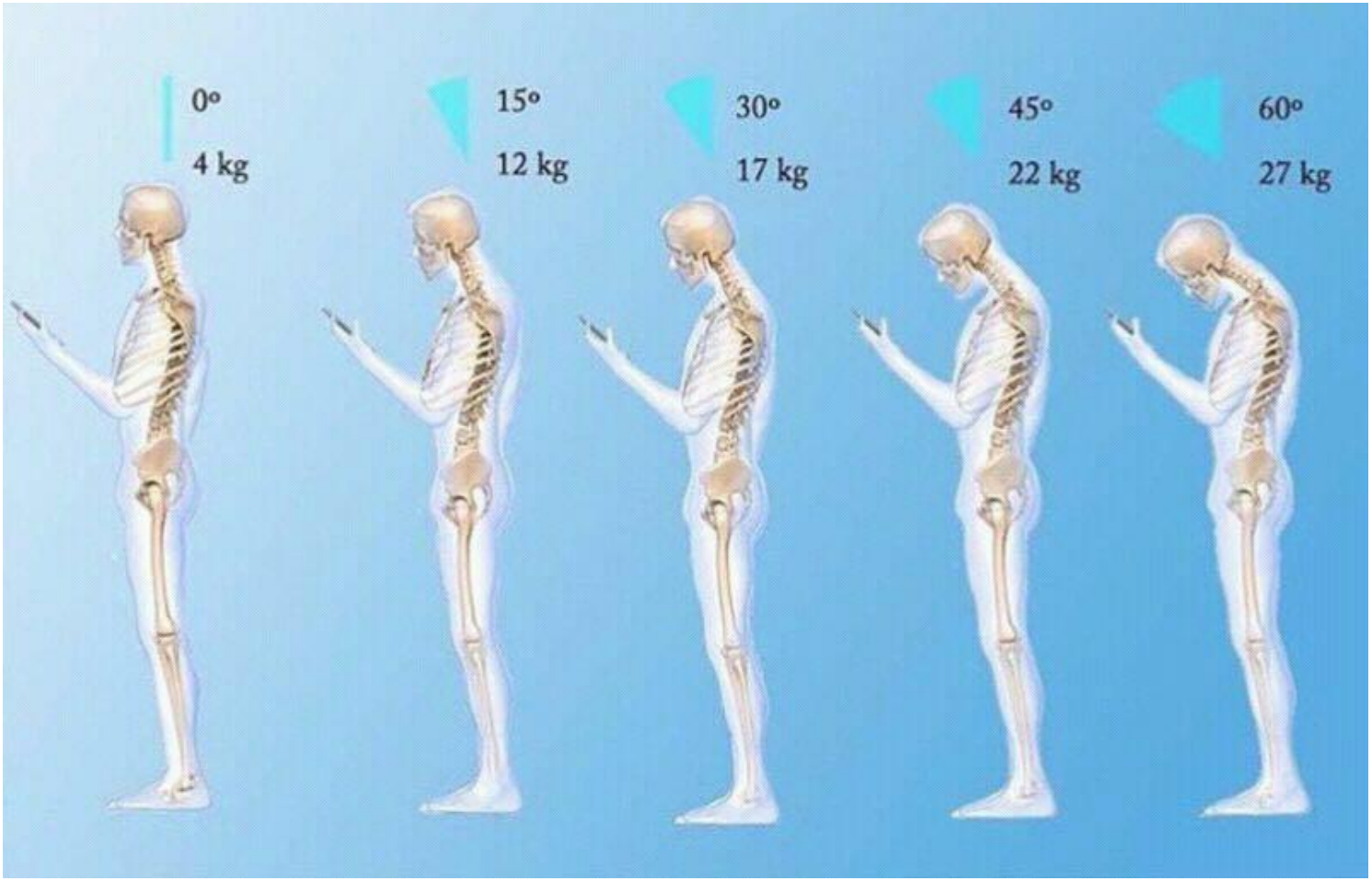
- **1. Strong passwords**
- **“We always recommend strong passwords that include upper case letters and lower case letters.**
- **“40% of people in Cleveland use the same passwords for each online account.**
- **“Once they get in they are laughing. They can change the password so the person can’t get in.”**
- **2. Don’t treat it as a popularity contest**
- **On one social media platform, a 12-year-old girl had 7,000 followers.**
- **“She was just accepting every friend request she received.**
- **“These people send requests because they want to abuse that permission.”**
- **3. Think before you post**
- **“Once the picture goes online you’ve no chance of getting it back.**
- **“Even if you take the original down, you don’t know if someone has screen shotted it.”**
- **4. Keep on top of your security settings**
- **If you share your images, be aware of what your security settings are.**
- **Take Snapchat for example - the blue ‘hotspots’ on the Snap Map function mean you can see anyone’s story that is in that particular area.**
- **If you change your security settings, the story will not be visible to the public.**

All your peripheral Devices

- **Check all your peripheral Digital Devices to be updated**
- **Copier**
- **Scaner**
- **Printers etc**

Neck and Neck problem

- Did you know that your head weighs around 04 or 05 kg? All supported by some pretty small bones in your neck! A Quick look at biomechanic of the body shows that when you are slouched over a phone at 45 degree angle.its equivalent to placing 22kg of stress on the neck! This often translates into headache and pain down the back....consider your posture!


0°
4 kg
15°
12 kg
30°
17 kg
45°
22 kg
60°
27 kg


T.H.I.N.K.
b4 u Send
Apply the T.H.I.N.K. test before posting or sending a cyber-message or photo, ask yourself:
T. is it true?
H. is it hurtful?
I. is it illegal?
N. is it necessary?
K. is it kind?

Indian Cyber Laws

Indian Cyber Laws were official 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.

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.

Testimonial Compulsion

- Case Laws:

1. Nandini Satpathy vs Dani (P.L.) And Anr on 7 April, 1978
2. Identification of prisoners act,1920
3. Selvi & Ors vs State Of Karnataka & Anr on 5 May, 2010

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.”

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

Evidentiary Value

Certificate u/s 65B of Indian Evidence Act

Banker's Books Evidence Act

- section 138 of the Negotiable Instruments Act for the cheque "bouncing".
- Ram has requested Indian Bank Ashok nagar Branch for a certified copy of Sameer's bank account statement (for January 2008) for producing in court as evidence. The printout of the bank statement will be accompanied by three certificates.

Admissibility: Before Court

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

Admissibility of Digital 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. In Amitabh Bagchi vs. Ena Bagchi (AIR 2005 Cal 11)

- [Sections 65-A and 65-B of Evidence Act, 1872 were analyzed.]
- The court held that the physical presence of person in Court may not be required for purpose of adducing evidence and the same can be done through medium like video conferencing.
- Sections 65-A and 65-B provide provisions for evidences relating to electronic records includes videoconferencing.

2. 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.**

3. 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.**

4. 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!**

5. 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**

6. 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).

7.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 Trail.**
- **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.**

8.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.**

9.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.**

10.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**

11.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

12.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.

13.Dhariwal Industries Ltd. vs. Kishore Wadhwani & 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

CDRs and E Records Case Laws

- **14. CALL RECORDS**

  Rakesh Kumar and Ors. V State, the High Court of Delhi

- In Bombay Bomb Blast case Sanjay Dutt CDR were admitted and the same were in Parliament Attack case

15. Electronic records

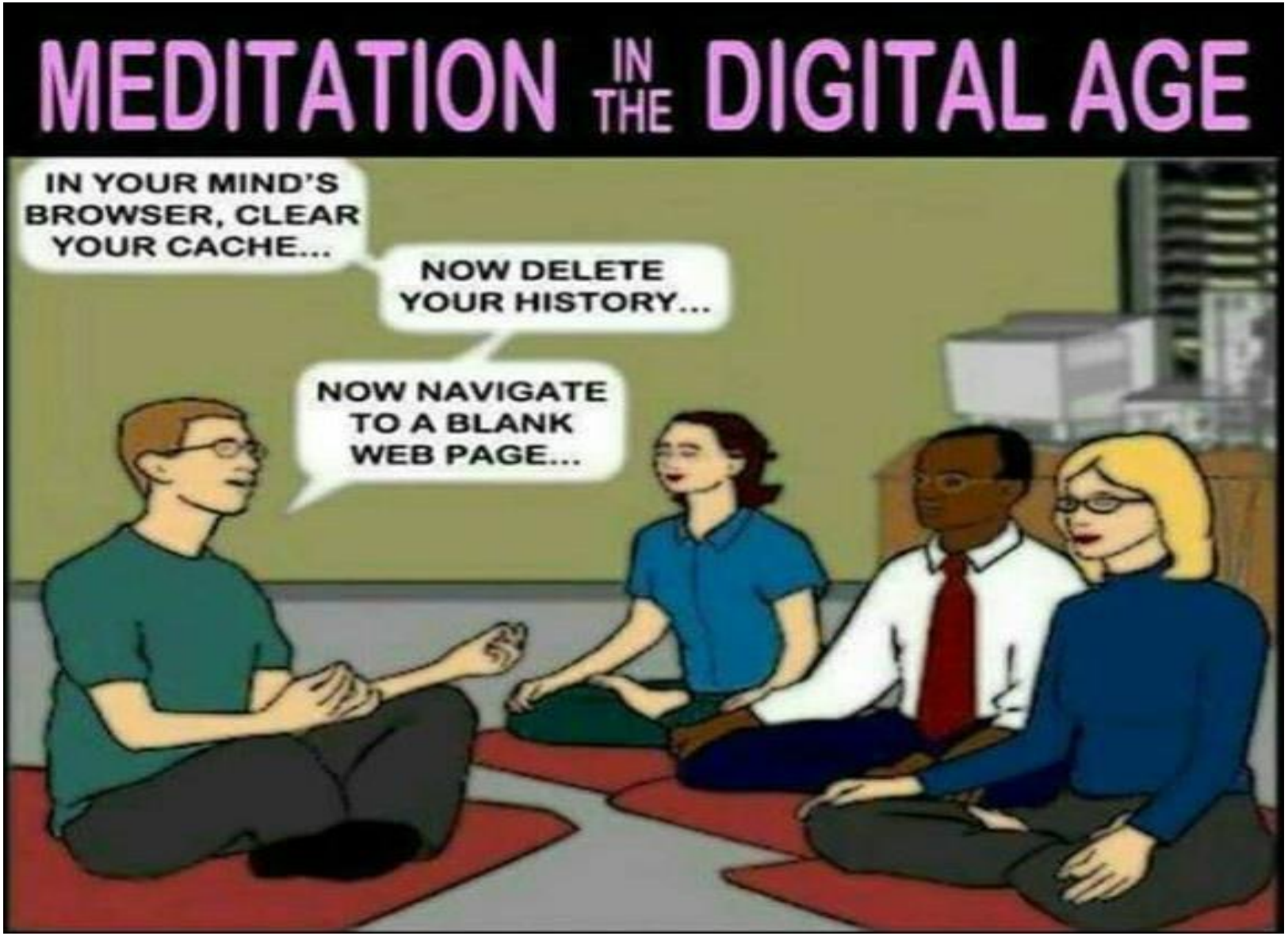
K.K. Velusamy Vs. N. Palanisamy, 2011 EQ–SC–0–158 SCI

16. Moninder Singh Pandher and Surendra Koli v State of U.P. (Criminal)

- **(Appeal No. 1475 of 2009), the question arose as, to admissibility of the confessional**
- statement which was recorded in video, as there is no provision for video recording of the confessional statement The High Court further relied on S 65B of the Evidence Act and held that the confession was admissible

17.R.K. Anand Vs.Registrar, Delhi High Court, (2009) 8 SCC 106.

- **Tape Record Admissibility conditions various conditions for admissibility of a tape-recorded statement were reiterated**
- **18.Tukaram S. Dighole Vs Manikrao Shivaji Kokate (2010) 4 SCC 329**
- **"Standard of proof" in the form of electronic evidence should be "more accurate and stringent" compared to other documentary evidence**


MEDITATION IN THE DIGITAL AGE
IN YOUR MIND'S BROWSER, CLEAR YOUR CACHE...
NOW DELETE YOUR HISTORY...
NOW NAVIGATE TO A BLANK WEB PAGE...


Resolve to be more secure in 2018
Have strong passwords & never share them with anyone
Protect corporate data and devices
Do not open unknown URLs or attachments
Back up all confidential files regularly
Do not post corporate information on social media
Use antivirus and update it regularly
Report any information security incident
Wish you a Happy, Prosperous & Cyber Safe 2018


Question
Time

Contact me @….

- **919444049224**

drsmurugan.tnpol@gov.in

muruganips@gmail.com

Thank you