

Techno-Legal session on:

**“Cyber Crimes & its investigation
and dealing with electronic
evidence in court room”**

By Bivas Chatterjee

New Trends in Evidence

1) Germanwings crash: Co-pilot researched suicide methods, cockpit doors:

Analysis of a tablet device belonging to Germanwings Flight 9525 co-pilot Andreas Lubitz shows he researched suicide methods on the Internet in the days leading up to the crash.

Police analysis of the correspondence and search history on the device, retrieved from Lubitz's Dusseldorf apartment, demonstrated that the co-pilot used it from March 16 to March 23.

Lubitz is suspected of deliberately bringing down Germanwings Flight 9525 in the French Alps on March 24, killing all 150 on board. Investigators have since focused on his health as they try to establish his motivation.

(<https://edition.cnn.com/2015/04/02/europe/france-germanwings-plane-crash-main/index.html>)

Cops use murdered woman's Fitbit to charge her husband:

A masked intruder barged into his Connecticut home, he said, tied up and tortured him and -- when his wife came home -- shot and killed her.

His story, however, would not hold up with investigators. And when cops ultimately charged *him* with murdering his wife, they relied on evidence gathered from an unlikely source:

- ❖ **The Fitbit his wife was wearing.**
- ❖ **At 9:01 a.m. Richard Dabate logged into Outlook from an IP address assigned to the internet at the house.**
- ❖ **At 9:04 a.m., Dabate sent his supervisor an e-mail saying an alarm had gone off at his house and he's got to go back and check on it.**
- ❖ **Connie's Fitbit registered movement at 9:23 a.m., the same time the garage door opened into the kitchen.**
- ❖ **Connie Dabate was active on Facebook between 9:40 and 9:46 a.m., posting videos to her page with her iPhone. She was utilizing the IP address at their house.**
- ❖ **While she was at home, her Fitbit recorded a distance of 1,217 feet between 9:18 a.m. and 10:05 a.m. when movement stops.**

(<https://edition.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html>)

Suspect OKs Amazon to hand over Echo recordings in murder case

Alexa, can you help with this murder case?

<https://edition.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/index.html>

Cyber Threats

India has bypassed Japan to become the world's third largest Internet user after China and the United States.

❖ Three-fourths of India's online population is under 35 as against just over half worldwide, the comScore report, India Digital Future in Focus 2013.

❖ As per the Telecom Regulatory Authority of India (TRAI), the number of Internet subscribers in India are 164.81 million as of March 31, 2013, with seven out of eight accessing the Internet from their mobile phones.

❖ As per TRAI Report, 2015 India has 997 million telecom Subscribers, 99.20m broadband subscribers, 300m subscribers accessing internet, 93% are through wireless media, 7% through fixed wire line media.

❖ Hon'ble Supreme Court of India in Dr. Subramanian Swamy vs. Election Commission of India on 8th October, 2013. ——— Hacking the E-Voting System.

Latest NCRB Data, 2015:

1) Increase of Cyber Crimes in 2015 compared with the previous year: 21.6% (In West Bengal : 12.1%) (No. of Crimes Reported in 2015: 11331)(In West Bengal : 398).

2) Increase in Arrest in Cyber Crime cases in 2015 compared with the previous year: 42.5% (In West Bengal: 35%), (No. of person arrested in Crimes Reported in 2015: 8044).(In West Bengal : 287).

3) Total No. person under trial: Male: 10295, Female: 239. Person Convicted: Male : 300, Female : 2. Acquitted: 519.

4) Age Group: Highest age group: 18 < > 30.

Gary McKinnon (born 10 February 1966) is a Scottish systems administrator and hacker who was accused in 2002 of perpetrating the "biggest military computer hack of all time," although McKinnon himself states that he was merely looking for evidence of free energy suppression and a cover-up of UFO activity and other technologies potentially useful to the public.

(https://en.wikipedia.org/wiki/Gary_McKinnon)

Challenges

i) Encryption nightmare of LEA:

: Use of IMs by Terrorists

ii) Dark web attack & Crypto Currency:

a) .onion b) @Signait

c) Ransomware d) BTC

iii) Growing use of Cloud & Cloud not forensics friendly.

iv) Difficulties in transfer of information by Intermediaries abroad.

v) VOIP Call & SIP

Encryption

Two Way sword

: End to End encryption used by terrorist groups

: ISIS Case in India: Use of Telegram.

Indian Penal Code

In section 118, In for the words

“Voluntarily conceals by any act or illegal omission, the existence of a design”, the words “Voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design “ shall be substituted.

In section 119, In for the words “Voluntarily conceals by any act or illegal omission, the existence of a design”, the words “Voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design “ shall be substituted;

DARK-WEB : TOR: .ONION

Two Recent Cases

Ransomware : use of .onion

Use of waytobehidden@Signaint

Harvard University Case: FBI agents tracked Harvard bomb threats despite Tor :

<http://www.theverge.com/2013/12/18/5224130/fbi-agents-tracked-harvard-bomb-threats-across-tor>

WELCOMING CHALLENGES

- **EXPERIMENTING ATTITUDE**
- **TECHNO-LEGAL KNOWLEDGE ACQUISITION :**
- **CODING : 1) ANY ONE LANGUAGE: MAY BE PYTHON & JAVASCRIPT**
- **2) MAY BE A MEMBER OF CODING COMMUNITY**
- **THINK FROM THE MIND OF AN DEFENCE LAWYER.**
- **CAN NOT DEAL ON THE SUSPECT DEVICE**
- **DOCUMENT EVERY STEP IN THE ROAD MAP OF THE ELECTRONIC EVIDENCE.**
- **TAKE HELP OF SECTION 27 & 8 OF IEA IN CASE THE TECH-SAVVY ACCUSED IS ONLY AWARE OF THE MODUS AND MOTIVE OF TECH-CRIME.**

- **LOCARD'S EXCHANGE PRINCIPLE:**
- **PAUL L. KIRK EXPRESSED THE PRINCIPLE AS FOLLOWS:**
- **"WHEREVER HE STEPS, WHATEVER HE TOUCHES, WHATEVER HE LEAVES, EVEN UNCONSCIOUSLY, WILL SERVE AS A SILENT WITNESS AGAINST HIM. NOT ONLY HIS FINGERPRINTS OR HIS FOOTPRINTS, BUT HIS HAIR, THE FIBERS FROM HIS CLOTHES, THE GLASS HE BREAKS, THE TOOL MARK HE LEAVES, THE PAINT HE SCRATCHES, THE BLOOD OR SEMEN HE DEPOSITS OR COLLECTS. ALL OF THESE AND MORE, BEAR MUTE WITNESS AGAINST HIM. THIS IS EVIDENCE THAT DOES NOT FORGET. IT IS NOT CONFUSED BY THE EXCITEMENT OF THE MOMENT. IT IS NOT ABSENT BECAUSE HUMAN WITNESSES ARE. IT IS FACTUAL EVIDENCE. PHYSICAL EVIDENCE CANNOT BE WRONG, IT CANNOT PERJURE ITSELF, IT CANNOT BE WHOLLY ABSENT. ONLY HUMAN FAILURE TO FIND IT, STUDY AND UNDERSTAND IT, CAN DIMINISH ITS VALUE."**
- **IN FORENSIC SCIENCE, LOCARD'S EXCHANGE PRINCIPLE HOLDS THAT THE PERPETRATOR OF A CRIME WILL BRING SOMETHING INTO THE CRIME SCENE AND LEAVE WITH SOMETHING FROM IT, AND THAT BOTH CAN BE USED AS FORENSIC EVIDENCE. DR. EDMOND LOCARD, A PIONEER IN FORENSIC SCIENCE HAD FORMULATED THE BASIC PRINCIPLE OF FORENSIC SCIENCE AS: "EVERY CONTACT LEAVES A TRACE"**
- **[[HTTPS://EN.WIKIPEDIA.ORG/WIKI/LOCARD%27S_EXCHANGE_PRINCIPLE](https://en.wikipedia.org/wiki/Locard's_exchange_principle)]**
- **THE PRINCIPLE IS SOMETIMES STATED AS "EVERY CONTACT LEAVES A TRACE", AND APPLIES TO CONTACT BETWEEN INDIVIDUALS AS WELL AS BETWEEN INDIVIDUALS AND A PHYSICAL ENVIRONMENT.**

এবার রাজ্যেও হানা দিল ‘ডার্ক ওয়েব’

সাইবার-দস্যুদের খপ্পরে পড়ে চুরি গেল মালদহের সরকারি দপ্তরের তথ্য

চিত্রদীপ চক্রবর্তী

ডার্ক ওয়েব কী ?



» টর ব্রাউজার ব্যবহার করে
অপরাধ করাই ডার্ক ওয়েব
অ্যাটাক

» সুপারি কিলার থেকে হেরোইন
সবই বিক্রি হয় এখানে

» এখন ডেটা চুরি করে বিক্রি
করা হয় এখান থেকে

» বিনিময়ে দাবি করা হয় মোটা
টাকা

» অপরাধীদের খুঁজে পাওয়া কার্যত অসম্ভব

আইপি অ্যাড্রেস তৈরি করে এ সব অপরাধমূলক কাজকর্ম করা হয়।

এখানকার যাবতীয় তথ্য এনক্রিপ্টেড করে রাখায়, তা চট করে উদ্ধার করাও যায় না। বিভাস চট্টোপাধ্যায়ের বক্তব্য, ‘আমরা ইন্টারনেট ব্যবহার করে এই ধরনের ক্ষেত্রে মাত্র চার শতাংশ অ্যাকসেস পেতে পারি। বাকি ৯৬ শতাংশ ডার্ক এলাকাতেই থেকে যায়। ফলে বেশির ভাগ সময়েই নানা রকম ছদ্ম আইপি-র খোঁজ পাওয়া যায়। যা দিয়ে অপরাধীকে ধরা সম্ভব হয় না। একমাত্র হার্ভার্ড বিশ্ববিদ্যালয়ের ক্ষেত্রে একটি ঘটনায় তাদেরই এক ছাত্রকে

গ্রেপ্তার করা সম্ভব হয়েছিল। কারণ সে নিজেদের বিশ্ববিদ্যালয়ের কম্পিউটারই ব্যবহার করেছিল।’

মালদহের ঘটনাটি কী করে জানা গেল? একটি সরকারি দপ্তরে চলতি মাসের প্রথম দিকে কম্পিউটার খুলে কাজ করার সময়ে একটি পপআপ ভেসে ওঠে। সেখানে ক্লিক করার সঙ্গে সঙ্গেই অধিকাংশ ডেটা চুরি হয়ে যায়। এর পরেই উল্টোদিক থেকে মোটা টাকা দাবি করা হয়। প্রথম দিকে পুলিশকর্তারা বিষয়টি বুঝতে না-পারলেও, পরে তথ্যপ্রযুক্তি বিশেষজ্ঞদের সাহায্য নেন। তাঁরাই তদন্তে নেমে জানতে পারেন, প্রায় দশ ডিজিটের একটি সংখ্যার পরে ডট ওনিনয় নামে একটি ওয়েবসাইট থেকে ওই সরকারি তথ্যগুলি হ্যাক করে নেওয়া হয়েছে।

কিন্তু সেই ওয়েবসাইটের আইপি নম্বরের হদিস পাওয়া যায়নি। তবে ওই সরকারি দপ্তরের সতর্কতায় বড়সড় বিপর্যয় এড়ানো গিয়েছে। কারণ, ওই কম্পিউটারে কুইক হিলস নামে একটি অ্যান্টি ভাইরাস লোড করা ছিল, যারা সমস্ত তথ্যর ব্যাকআপ রেখে দিয়েছিল। ফলে কয়েক দিনের মধ্যে পুরোনো যাবতীয় তথ্য ফিরে পাওয়া যায়। তথ্যপ্রযুক্তি বিশেষজ্ঞদের মতে, এই হ্যাকারদের হানা এর আগে পশ্চিমবঙ্গে দেখা যায়নি। তবে সীমান্ত ঘেঁষা মালদহ জেলায় এর থাবা যথেষ্ট চিন্তার। ভবিষ্যতে এমনও হতে পারে, কারও নেটব্যাকিং সিস্টেম হ্যাক করে ডার্ক ওয়েব অ্যাটাকাররা মোটা টাকা চেয়ে নিতে পারে। আন্ডারওয়ার্ল্ডে এখনও এ ভাবেই তোলা আদায়ের কাজ করা হয়। সেই টাকা খাটানো হয় বিভিন্ন ব্যবসায়। যার কোনও হদিস কেউ পায় না।

দিতে হবে ৩ বিট কয়েন।

মানে ভারতীয় মুদ্রায় প্রায় দু’লক্ষ টাকা। কিন্তু সেটা আবার নগদ বা ব্যাঙ্ক অ্যাকাউন্টে ট্রান্সফার করলে চলবে না। পেমেন্ট হবে ক্রিপ্টো কারেন্সিতে। যা কি না সাইবার স্পেসে ভেসে থাকা একটি ওয়ালেট। মালদহের ইংরেজবাজারের রাজ্য সরকারের দপ্তরে কি তা হলে হানা দিল অদৃশ্য তোলাবাজ? পুলিশকর্তারা যখন হন্যে হয়ে এর সূত্র খুঁজে বেড়াচ্ছেন, তখনই জানা যায় ওই কম্পিউটারে নীরবে ঘটে গিয়েছে ‘ডার্ক ওয়েব অ্যাটাক’। আমেরিকা-সহ বিশ্বের বিভিন্ন দেশে এর আগে এ ধরনের ঘটনা ঘটলেও, পশ্চিমবঙ্গে এই প্রথমবার হানা দিয়েছে এই অদৃশ্য নেটদস্যুরা। সাইবার ক্রাইম বিশেষজ্ঞ বিভাস চট্টোপাধ্যায়ের বক্তব্য, ‘এই আড়ালে থাকা অপরাধীদের খুঁজে বের করা কার্যত অসম্ভব। কারণ, এই মুহূর্তে ভারতে তো পরক্ষণেই বিদেশের কোনও প্রত্যন্ত গ্রামে হয়তো খুঁজে পাওয়া যাবে এই দুষ্টীদের আইপি অ্যাড্রেস। আর টাকার হদিস তো পাওয়াই যাবে না। এত দিন আন্ডারওয়ার্ল্ডে এই প্রযুক্তি ব্যবহার করলেও, এখন মালদহের মতো শহরেও প্রয়োগ করা হচ্ছে এই প্রযুক্তি।’

কিন্তু এর নেপথ্যে আসল খেলা কার? বিশেষজ্ঞদের মতে, এই খেলার আসল খেলোয়াড় ‘টর’ নামে একটি ব্রাউজার। অনেক দেশ এই ব্রাউজারটিকে ইতিমধ্যেই নিষিদ্ধ করে দিয়েছে। কিন্তু এ দেশে তা চলছে। এই ব্রাউজার ব্যবহার করলে নর্মাল ব্রাউজার দিয়ে তার হদিস পাওয়া যায় না। ফলে নকল

Section 9 of Indian Evidence Act, 1872. Facts necessary to explain or introduce relevant facts.-Facts necessary to explain or introduce a fact in issue or relevant fact, or which support or rebut an inference suggested by a fact in issue or relevant fact, or which establish the identity of any thing or person whose identity is relevant, or fix the time or place at which any fact in issue or relevant fact happened, or which show the relation of parties by whom any such fact was transacted, are relevant in so far as they are necessary for that purpose.

হাতের ছাপে কোটির প্রতারণা

হিমাদ্রি সরকার

সেকেন্ড হ্যান্ডে কেনার জন্য টাকা দিয়েছিলেন তিনি। কিন্তু মোবাইল হাতে পাননি। প্রতারণার অভিযোগে তদন্ত শুরু করে পুলিশ। সে তদন্ত করতে গিয়েই কেঁচো খুঁড়তে কেউটে বেরিয়ে আসে। যে অ্যাকাউন্টে টাকা মিটিয়েছিলেন শিবম, সেই অ্যাকাউন্টের সূত্র ধরেই ধাপে ধাপে বুবাইয়ের নাগাল পান তদন্তকারীরা। বুবাইকে জেরা করে পুলিশ জানতে পারে, আঙুলের ছাপ জালিয়াতি করে অভিনব কায়দায় প্রতারণার কারবার ফেঁদে বসেছিল সে। এই মামলায় বিশেষ সরকারি আইনজীবী বিভাস চট্টোপাধ্যায়ের কথায়, 'ব্যাঙ্ক অ্যাকাউন্ট সুরক্ষিত রাখতেই আঙুলের ছাপ নেওয়ার ব্যবস্থা। কিন্তু সেখানেই যে ভাবে প্রতারণার জাল ছড়িয়েছে অভিযুক্ত, তা নজিরবিহীন। ইন্ডিয়ান এন্ডিডেল অ্যাক্টের ন'নম্বর ধারা অনুযায়ী অপরাধী শনাক্তকরণ প্যারেডের মতো আদালতে তথ্য শনাক্তকরণ প্যারেডের আর্জি জানানো হয়েছিল। আদালত সে আর্জি মঞ্জুর করে। যাঁদের নামে অ্যাকাউন্ট খোলা হয়েছিল তাঁদের ও বুবাইয়ের আঙুলের ছাপ শনাক্ত করা হয়েছে।' সাইবার অপরাধের ঘটনায় এ ভাবে আদালতে সাক্ষ্য হাজির করাও

উদয় দেব



নজিরবিহীন বলে মত বিশেষজ্ঞদের।

কী ভাবে চলছিল এই কারবার?

পুলিশ সূত্রের খবর, প্রধানমন্ত্রীর জনধন প্রকল্পের আওতায় ১০০ শতাংশ মানুষের ব্যাঙ্ক অ্যাকাউন্ট খোলার যে উদ্যোগ ব্যাঙ্কগুলি নিয়েছে, তারই ফাঁক গলে প্রতারণার জাল ছড়িয়েছিল বুবাই। গ্রামীণ এলাকায় রাষ্ট্রায়ত্ত্ব ব্যাঙ্কগুলির হয়ে বেসরকারি এজেন্টরা গ্রাহকের অ্যাকাউন্টের জন্য নথিপত্র জমা নেন। এঁদের বলা হয় 'ব্যাঙ্কমিত্র'। এই অ্যাকাউন্ট খুলতে গ্রাহকের ১০ আঙুলের মধ্যে যে কোনও দুই আঙুলের ছাপ ও স্বাক্ষর লাগে। তদন্তকারীরা জানান, বুবাইও এ ভাবেই এজেন্ট হিসাবে কাজ করতে গিয়ে গ্রাহকদের নথিপত্র জমা নেয়। তার পর অ্যাকাউন্ট খুলতে যে

আঙুলের ছাপ ও স্বাক্ষর লাগে সেখানে গ্রাহকের পরিবর্তে নিজেরই আঙুলের ছাপ বসিয়ে দেয়। অর্থাৎ ভবিষ্যতে কোনও গ্রাহকের নামে অ্যাকাউন্ট খোলা হলেও অ্যাকাউন্টের আসল চাবিকাঠি থেকে যায় তার হাতেই। এ ভাবে একটি রাষ্ট্রায়ত্ত্ব ব্যাঙ্কে অনেকগুলি ভুয়ো অ্যাকাউন্ট খোলে বুবাই। এর পাশাপাশি পুরোনো জিনিসপত্র অনলাইনে কেনাবেচার

একটি সাইটেও অ্যাকাউন্ট খোলে সে। সেখানে বিভিন্ন নামী সংস্থার দামি মোবাইল সেকেন্ড হ্যান্ডে অর্ধেক দামে বিক্রি করবে বলে বিজ্ঞাপন দেয়। তাতে শর্ত ছিল, কেউ ওই মোবাইলটি বুক করলে কিছু টাকা অগ্রিম দিতে হবে। পার্সেল করে সেই মোবাইলটি ডেলিভারির জন্য গেলে মিটিয়ে দিতে হবে বাকি টাকা। এই বিজ্ঞাপন দেখেই শিবমের মতো অনেক গ্রাহক সন্তায় মোবাইল কেনার লোভে অনলাইনে বিভিন্ন অ্যাকাউন্টে টাকা জমা দেন। সেই টাকা জমা পড়ত বুবাইয়ের আঙুলের ছাপ ব্যবহার করে তৈরি ব্যাঙ্ক অ্যাকাউন্টেই। টাকা জমা পড়লেই ব্যাঙ্কে গিয়ে নিজের আঙুলের ছাপ ব্যবহার করে সে টাকা নিমেষে হাপিস করে দিত বুবাই।

তদন্তে নেমে প্রথমে যাঁদের নামে অ্যাকাউন্ট খোলা হয়েছিল, তাঁদের বাড়িতে হানা দেয় পুলিশ। নিরীহ গ্রাহকরা আকাশ থেকে পড়েন। তাঁরা জানান, অ্যাকাউন্ট খোলার সময়ে তাঁদের আঙুলের ছাপ নেওয়াই হয়নি। এর পর যে সংস্থাটি অ্যাকাউন্ট খোলার কাজ করছিল, তাদের সূত্র ধরেই হদিস মেলে আসল প্রতারকের। প্রতারণার টাকাতই দামি গাড়ি, বাড়ি হাঁকিয়েছিল বুবাই।

বয়স মাত্র কুড়ির আশপাশে। বাড়ির বিভিন্ন কোণে অন্তত ৩৬টি ক্লোজড সার্কিট ক্যামেরা বসানো। গ্যারাজে সাজানো তিন-লাখি বাইক। সে ছেলের কারবারে রীতিমতো চক্ষুচড়কগাছ দুঁদে গোয়েন্দাদের। প্রায় সওয়া কোটি টাকা প্রতারণার অভিযোগে আপাতত জেল হাজতে বছর কুড়ির বুবাই ঘোষ। যে কায়দায় দেশের বিভিন্ন রাজ্যের কয়েকশো লোককে সে প্রতারণার ফাঁদে ফেলেছে, তা বুঝে উঠতে কার্যত হিমসিম খাচ্ছেন তদন্তকারীরা। বাঁকুড়ার প্রত্যন্ত সোনামুখী এলাকার কলেজ পড়ার মাথায় যে এত বুদ্ধি থাকতে পারে, তা-ও তাঁদের ধারণার বাইরে। আপাতত ছেলেটিকে জেরা করে প্রতারণার জাল ছাড়াতে ব্যস্ত তদন্তকারীরা।

কী ভাবে এই প্রতারণার কারবার নজরে এল পুলিশের?

মাস কয়েক আগের কথা। উত্তরপ্রদেশের জৌনপুরের বাসিন্দা শিবম জয়সওয়াল যোগাযোগ করেন বাঁকুড়ার বিষ্ণুপুরের এসডিপিও লাল্টু হালদারের সঙ্গে। অনলাইন বিপণনের একটি ওয়েবসাইটে দামি মোবাইল

Section 79A of IT Act

Explanation:

"Electronic Form Evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines".

**Frye vs. United States, 293 F. 1013: Admissibility of Scientific Evidence:
Expert opinion based on scientific technique
is admissible only where the technique
is generally accepted as reliable in the relevant scientific community.**

**Dauber vs. Merrell Dow Pharma., 509 U.S.579(1993): Supreme Court ruled
that the Federal Rules of Evidence superseded Frye as the standard for
admissibility of expert evidence in federal court.**

**Rule 702 of the Federal Rules of Evidence provides (in part):
If scientific, technical, or other specialized knowledge will assist the trier
of fact to understand the evidence or to determine a fact in issue, a
witness qualified as an expert by knowledge, skill, experience, training, or
education, may testify thereto in the form of an opinion or otherwise...**

**“Evidence” .— “ Evidence” means and includes—(1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, such statements are called oral evidence;
(2) ⁶ [all documents including electronic records produced for the inspection of the Court], such documents are called documentary evidence.**

“electronic form”, “electronic records”, “information”, “secure electronic record”, “secure digital signature” and “subscriber” shall have the meanings respectively assigned to them in the Information Technology Act, 2000 (21 of 2000).]

- **2(K)"COMPUTER RESOURCE" MEANS COMPUTER, COMPUTER SYSTEM, COMPUTER NETWORK, DATA, COMPUTER DATA BASE OR SOFTWARE;**
- **(L)"COMPUTER SYSTEM" MEANS A DEVICE OR COLLECTION OF DEVICES, INCLUDING INPUT AND OUTPUT SUPPORT DEVICES AND EXCLUDING CALCULATORS WHICH ARE NOT PROGRAMMABLE AND CAPABLE OF BEING USED IN CONJUNCTION WITH EXTERNAL FILES WHICH CONTAIN COMPUTER PROGRAMMES, ELECTRONIC INSTRUCTIONS, INPUT DATA AND OUTPUT DATA THAT PERFORMS LOGIC, ARITHMETIC, DATA STORAGE AND RETRIEVAL, COMMUNICATION CONTROL AND OTHER FUNCTIONS;**

- **2(O)"DATA" MEANS A REPRESENTATION OF INFORMATION, KNOWLEDGE, FACTS, CONCEPTS OR INSTRUCTIONS WHICH ARE BEING PREPARED OR HAVE BEEN PREPARED IN A FORMALISED MANNER, AND IS INTENDED TO BE PROCESSED, IS BEING PROCESSED OR HAS BEEN PROCESSED IN A COMPUTER SYSTEM OR COMPUTER NETWORK, AND MAY BE IN ANY FORM (INCLUDING COMPUTER PRINTOUTS MAGNETIC OR OPTICAL STORAGE MEDIA, PUNCHED CARDS, PUNCHED TAPES) OR STORED INTERNALLY IN THE MEMORY OF THE COMPUTER;**
- **(R) "ELECTRONIC FORM", WITH REFERENCE TO INFORMATION, MEANS ANY INFORMATION GENERATED, SENT, RECEIVED OR STORED IN MEDIA, MAGNETIC, OPTICAL, COMPUTER MEMORY, MICRO FILM, COMPUTER GENERATED MICRO FICHE OR SIMILAR DEVICE;**

- **(V) "INFORMATION" INCLUDES¹² [DATA, MESSAGE, TEXT], IMAGES, SOUND, VOICE, CODES, COMPUTER PROGRAMMES, SOFTWARE AND DATA BASES OR MICRO FILM OR COMPUTER GENERATED MICRO FICHE.**
- **'(J) "COMPUTER NETWORK" MEANS THE INTERCONNECTION OF ONE OR MORE COMPUTERS THROUGH-**
- **(I) THE USE OF SATELLITE, MICROWAVE, TERRESTRIAL LINE OR OTHER COMMUNICATION MEDIA; AND**
- **(II) TERMINALS OR A COMPLEX CONSISTING OF TWO OR MORE INTERCONNECTED COMPUTERS WHETHER OR NOT THE INTERCONNECTION IS CONTINUOUSLY MAINTAINED;'**

**1) Justice Stephen Breyer of the US Supreme Court —“Science in the Courtroom”,
“In this age of science, science should expect to find a warm welcome, perhaps a permanent home, in our courtrooms... Our decisions should reflect a proper scientific and technical understanding so that the law can respond to the needs of the public.”**

**2) In Daubert Merrel Dow Pharmaceuticals Inc, the American Supreme Court --
“...there are important differences between the quest for truth in the courtroom and the quest for truth in the laboratory. Scientific conclusions are subject to perpetual revision. Law, on the other hand, must resolve disputes finally and quickly.” Replied by our Hon’ble Supreme Court in A.P. Pollution Control Board vs. Prof M.V. Nayudu.**

3) In State of Maharashtra vs. Praful B. Desai (AIR 2003 SC 2053) the Hon;ble Supreme Court has observed that advancement in science and technology has also helped the process of law in administration of Justice.

As per section 2 (i) of IT Act, 2000 "Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

As per section 2(ha) of IT Act, 2000 "Communication Device" means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image.

"Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm; (b) that two electronic records can produce the same hash result using the algorithm.

Investigation

Section 4(1) and 4(2) of Cr.P.C. provide that the provisions of Cr.P.C. are equally applicable in cases relating to other offences which may include offences under Information Technology Act. The following are the special provisions which are having overriding effect with Cr.P.C. in case of police investigation.

Special Provisions in IT Act & ITA Act:

Section 76: Confiscation

Section 77A: Compounding of offences

Section 77B: Offence of Three years bailable

Section 78 :Investigation by Inspector and above

Section 80: Power to enter, Search, arrest without warrant any person who is reasonably suspected of committed or committing or about to commit any offence under this Act.

Section 84A : Modes or methods for encryption

Section 77: Compensation, penalties or confiscation not to interfere with other punishment.

**IN THE SUPREME COURT OF INDIA
CRIMINAL APPELLATE JURISDICTION
CRIMINAL APPEAL NO. 1222 OF 2016
(Arising out of S.L.P. (Criminal) No. 7675 of 2015)
Sharat Babu Digumarti ...Appellant(s)
Versus
Govt. of NCT of Delhi ...Respondent(s)**

“Once the special provisions having the overriding effect do cover a criminal act and the offender, he gets out of the net of the IPC and in this case, Section 292. It is apt to note here that electronic forms of transmission is covered by the IT Act, which is a special law. It is settled position in law that a special law shall prevail over the general and prior laws. When the Act in various provisions deals with obscenity in electronic form, it covers the offence under Section 292 IPC. “

Four steps to traceability

Traceability can be expressed in four independent steps.

First, one determines the IP address to be traced.

Second, one establishes which ISP (or perhaps a university) has been allocated the IP address.

Third, the ISP's technical records will indicate which user account was using the IP address at the relevant time.

Fourth and finally, the ISP's administrative records will establish the real-world" identity of the individual who was permitted to operate the account.

Investigation with websites: whois

<https://www.whois.com/>

Example : Code Level Investigation after whois analysis

OPEN SOURCE FORENSICS

FORENSICS ANALYSIS INVOLVES THE FOLLOWING STEPS:

- ❑ COLLECTION – SEARCH AND SEIZING OF DIGITAL EVIDENCE, AND ACQUISITION OF DATA.
- ❑ EXAMINATION – APPLYING TECHNIQUES TO IDENTIFY AND EXTRACT DATA.
- ❑ ANALYSIS – ANALYSIS BY USING DATA AND RESOURCES WITH STANDARD NORMS.
- ❑ REPORTING – PRESENTING THE REPORT.
- ❑ COMPUTER FORENSIC ANALYSIS CONSISTS OF THE FOLLOWINGS:
 - STORAGE MEDIA ANALYSIS
 - SOFTWARE SOURCE CODE ANALYSIS.
 - NETWORK TRAFFIC AND LOGS ANALYSIS.

ANDROID FORENSICS

ON OVERALL STUDY OF ANDROID ARCHITECTURE ESPECIALLY ITS SECURITY FEATURES IN THE FORM OF SANDBOXING, PERMISSION MODEL, ETC. ARE COMING IN THE WAY FOR A BETTER FORENSIC ANALYSIS OF THE TARGET SYSTEM. THERE ARE VARIOUS TYPES OF DATA ON ANDROID DEVICES NAMELY SMS, MMS, CHAT MESSAGES, BACKUPS, E- MAIL, CALL LOGS, CONTACTS, PICTURES , VIDEOS, BROWSER HISTORY, GPS DATA, DATA IN VARIOUS INSTALLED APPLICATION LIKE FACEBOOK, TWITTER, ETC. WHICH TODAY'S ANDROID FORENSIC EXPERTS ARE TO ANALYZE IN A VERY EFFICIENT WAY. AGAIN THERE ARE VARIOUS APPLICATIONS, SOME OF WHICH ARE COMING WITH ANDROID, SOME ARE INSTALLED BY THE MANUFACTURER OR WIRELESS CARRIER OR THE USER HIMSELF/ HERSELF. THESE APPLICATIONS AND THE DATA WITHIN ARE TO BE EXAMINED BY TODAY'S FORENSIC EXPERT. IMAGING AND ANALYZING THE ANDROID RAM OR MEMORY AND ACQUIRING THE ANDROID SD CARD IS ALSO AN IMPORTANT STEP IN ANDROID FORENSIC ANALYSIS. THE PROCESS OF RECOVERING THE DELETED DATA FROM THE INTERNAL ANDROID DEVICE AND SD CARD HAS ALSO BEEN DEVELOPED. IN ANDROID FORENSIC ANALYSIS, USER DICTIONARY ANALYSIS PROVIDES AN IMPORTANT SOURCE OF FORENSIC DATA. GMAIL ANALYSIS, GOOGLE CHROME ANALYSIS, GOOGLE MAP ANALYSIS, GOOGLE HANGOUT ANALYSIS, GOOGLE KEEP AND PLUS ANALYSIS, FACEBOOK AND FACEBOOK MESSENGER ANALYSIS, SKYPE, VIBER, WATSAPP, ETC ANALYSIS , ESPECIALLY RECOVERING THE VIDEO MESSAGES FROM SKYPE AND DECRYPTING THE WHATSAPP BACKUP ARE IMPORTANT STEP IN TODAY'S ANDROID FORENSIC ANALYSIS.

PYTHON ETC.....

FORENSIC INVESTIGATION USING JAVA OR PYTHON MAY BE OF GREAT HELP TO THE FORENSIC INVESTIGATOR IMPORTING SOCKET AND OTHER WAY. NOWADAYS IN MORE AND MORE CASES OF CLOUD COMPUTING, BIG DATA ANALYSIS, MOBILE APP DEVELOPMENT, NETWORK FORENSICS PYTHON CODE IS BEING USED. PYTHON PROGRAMMING IS OF GREAT USE IN PORT SCANNING, WEBSITE CLONING, WEB SERVER FINGER PRINTING, WIRELESS NETWORK SCANNING, ACCESSING MAIL SERVER, ETC. USING THE PYTHON AND GOOGLE API, THE LOCATION OF IP ADDRESSES CAN BE ANALYZED.

MICRO-PYTHON: IOT

LINUX BASE

- **AUTOPSY**
- **[HTTPS://WWW.SLEUTHKIT.ORG/AUTOPSY/](https://www.sleuthkit.org/autopsy/)**
- **PENETRATION TESTING WITH THE KALI LINUX DISTRIBUTION**
- **[HTTPS://WWW.KALI.ORG/](https://www.kali.org/)**
- **BE CAREFUL ABOUT SECTION 72A, 43, 43A OF ITA, 2000 AND OTHER PROVISIONS OF LAWS**
- **MUST HAVE SPECIFIC NDA-INDEMNITY SORT OF AGREEMENT**
- **FOR JUDICIAL MATTER : BY APPROPRIATE AUTHORITIES AND SPECIFIC SEARCH WARRANT: 4TH AMENDMENT, BILL OF RIGHT: USA**

- 1) Identity Theft**
- 2) Spam and Cyber Stalking**
- 3) Infringement of privacy**
- 4) Hacking-**
 - White Hat**
 - Black Hat**
 - Grey Hat**

Hacktivist

Hacktivism can be divided into two main groups:

- 1. Cyberterrorism**
- 2. Freedom of information**

5) Cyber Terrorism: - Terrorism in cyber world is cyberterrorism. Section 66F of the ITA Act, 2008 defines the word cyber terrorism in the following way:

“(1) whoever,-

(A) With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) Denying or cause the denial of access to any person authorised to access computer resource; or

(ii) Attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) Introducing or causing to introduce any Computer Contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.”

Important Cases on Cyber Terrorism

White Supremacist Movement —1996.

Institute of Global Communication Case –1998.

LTTE Attack Sri Lankan Embassy –1998.

Milworm hacked Bhabha Atomic Research Centre –1998.

Attack upon NATO computers —1999.

Chinese Code Red Virus – 2001.

Hacking U.S. Justice Departments –2001.

Pak Hacker attacked Eastern Railway Site-2008

26/11 Attack in India.

- 6) Child Pornography & Pornography**
- 7) Cyber Warfare**
- 8) Cyber Squatting**
- 9) Economic Espionage**
- 10) Software Piracy and other Copyright Violation**
- 11) Computer Forgery and Counterfeiting**
- 12) Virus / worm attacks**
- 13) Sabotage and Extortion by using Computer.**
- 14) Phishing and other Cyber Fraud**
- 15) Defamation, Hate Speech, Racist, Blogs and Xenophobic Propaganda**
- 16) Online Gambling**
- 17) Email Spoofing**
- 18) Data Dribbling**
- 19) Web Jacking**
- 20) Email Bombing**

Crime on Mobile Phones

In June, 3.7 million phones worldwide became infected with malware, Beijing researchers finds.

Mobile malware is rising fast, infecting nearly 13 million phones in the world during the year first half of 2012, up to 177% from the same period a year ago. This came as the security vendor found 5,582 malware programs designed for Android during the month, another unprecedented number for the period. (<http://www.computerworld.com>)

SELinux: Security Enhanced Linux

Mobile Platform Vulnerabilities and Risks

ØApp Stores

ØMobile Malware

ØOS and App Updates

ØMobile Application Vulnerabilities

ØPrivacy Issues (Geo-location)

ØData Security

ØExcessive Permissions

ØCommunication Security

ØPhysical Attacks

ØSecurity Issues arising from App Stores

ØInsufficient or no vetting of apps.

ØMalicious apps can damage other application and data and send your sensitive data to attackers.

ØThreats of Mobile Malware

ØMobile malware

App Sandboxing Issues

Sandboxing helps protect systems and users by limiting the resources the app can access in the mobile platform.

Jailbreaking removes sandbox restrictions, which enables malicious apps to access restricted mobile resources and information.

Android Trojan: ZitMo:

Zitmo is the notorious mobile component of the Zeus banking Trojan that circumvents two factors authentication by intercepting SMS confirmation codes to access bank accounts.

GingerBreak

Android OS/GingerBreak is a Trojan that affects mobile devices which drops and executes another trojan detected as Exploit.

AcnetSteal:

Trojan sends the contact information to a remote location using TripleDES Encryption (DESede).

Cawitt:

Cawitt operates silently in the background, gathering information like device ID, International Mobile Equipment Identity (IMEI) number, phone number, etc.

FakeToken:

FakeToken steals both banking authentication factors directly from the mobile device.

Phishing

Phishing scams are now a part of everyday life. It's important that you know how to spot one and avoid becoming a victim. Phishing scams are just another attempt to get valuable information. Scammers send a mass email to every address they can find. Typically the message will appear to come from a bank or financial institution.

Phishing Using Email

Phishing Using Phones

Phishing Using Surveys

Phishing Using Customer Authentication.

“The internet is an international network of interconnected computers.”

**The Supreme Court of United States of America (US)
in ACLU v. Reno, 521 US 844.**

Cyber Crimes are basically of three categories and they are:

Cyber Crimes against Property – Financial crimes – cheating on-line – illegal funds transfer.

Cyber Crimes against Persons – On-line harassment, Cyber Stalking, Obscenity.

Cyber Crimes against Nations – Cyber Terrorism – Damaging critical information infrastructures.

Cyber Laws In India

1) Information Technology Act, 2000.

2) Information Technology (Amendment Act), 2008.

3) Rules under Information Technology Act.

4) Amendment in Cr.P.C., Evidence Act and Indian Penal Code.

In the Statement of Objects and Reasons to the IT Act, it is stated:

“New communication systems and digital technology have made drastic changes in the way we live. A revolution is occurring in the way people transact business.”

Subject matter of Information Technology Act

Chapter – I Short Title, Extent, Commencement and Application and Definitions

Chapter – II Digital signature and Electronic Signature

CHAPTER III Electronic Governance

Chapter IV Acknowledgement and service

Chapter V Secure Record and Signature

Chapter VI Regulation of Certifying Authorities

Chapter VII Electronic Signature Certificates

Chapter VIII : Duties of Subscribers

Chapter IX of the said Act talks about penalties and adjudication for various offences.

Chapter X which envisage the Cyber Appellate Tribunal

Chapter XI of the said Act talks about various offences

Chapter: XII : Intermediaries

Chapter XIIA: Examiner of Electronic Evidence

Chapter XIII : Miscellaneous

6. Use of Electronic Records and Electronic Signature in Government and its agencies.-

(1) Where any law provides for -

(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(b) the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

7. Retention of Electronic Records -

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if -

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

7-A. Audit of Documents etc in Electronic form -

Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form.

8. Publication of rules, regulation, etc, in Electronic Gazette

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, bye-law, notification or any other matters published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

11. Attribution of Electronic Records -

An electronic record shall be attributed to the originator, -

- (a) if it was sent by the originator himself;**
- (b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or**
- (c) by an information system programmed by or on behalf of the originator to operate automatically.**

12. Acknowledgement of Receipt. -

(1) Where the originator has not agreed with stipulated that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by -

- (a) Any communication by the addressee, automated or otherwise; or**
- (b) Any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.**

13. Time and place of dispatch and receipt of electronic record. -

(1) Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely -

(a) If the addressee has designated a computer resource for the purpose of receiving electronic records, -

(i) Receipt occurs at the time when the electronic record enters the designated computer resource; or

(ii) If the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) If the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

Judgement on Section 11, 12 and 13 of the Information Technology Act, 2000:

The relevant landmark judgement in this respect is P.R. Transport Agency vs. Union of India in Civil Misc. Writ Petition No. 58468 of 2005 decided by High Court Of Allahabad which was decided on: 24.09.2005 and reported in AIR, 2006 All, 23 or 2006(1) AWC 504.

Section 13(3) of the Information Technology Act has covered this difficulty of “no fixed point either of transmission or of receipt”. According to this section “...an electronic record is deemed to be received at the place where the addressee has his place of business.”

The acceptance of the tender will be deemed to be received by PRTA at the places where it has place of business. In this case it is Varanasi and Chandauli both in U.P.

10-A. Validity of contracts formed through electronic means.-

Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

Jurisdiction

Section 75 of IT Act

75. Act to apply for offence or contraventions committed outside India.-

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

4. Extension of Code to extra-territorial offences.- The provisions of this Code apply also to any offence committed by-

(1) any citizen of India in any place without and beyond India;

(2) any person on any ship or aircraft registered in India wherever it may be.

(3) any person in any place without and beyond India committing offence targeting a computer resource locating in India.]

Explanation- In this section.-

(a) the word "offence" includes every act committed outside India which, if committed in India, would be punishable under this Code.

(b) the expression 'computer resource' shall have the meaning assigned to it in clause (k) of sub-section (1) of section 2 of the Information Technology Act, 2000 (21 of 2000)]

Banyan Tree Holding (P.) Ltd. V. A. Murali Krishnan Reddy & Anr, 2010 (42) PTC 361 (Del), has observed :

“At the outset, this court does not subscribe to the view that the mere accessibility of the Defendants’ website in Delhi would enable this Court to exercise jurisdiction. A passive website, with no intention to specifically target audiences outside the State where the host of the website is located, cannot vest the forum court with jurisdiction.”

“The learned single Judge in India TV acknowledged that a mere accessibility of website may not be sufficient to attract jurisdiction of the forum court. This, in the considered view of this Court, is the correct position in law.”

“A passive website, with no intention to specifically target audiences outside the State where the host of the website is located, cannot vest the forum court with jurisdiction. This court is therefore unable to agree with the proposition laid down in Casio. The said decision cannot be held to be good law and to that extent is overruled.”

“A mere hosting of an interactive web-page without any commercial activity being shown as having been conducted within the forum state, would not enable the forum court to assume jurisdiction. Even if one were to apply the „effects” test, it would have to be shown that the Defendant specifically directed its activities towards the forum state and intended to produce the injurious effects on the Plaintiff within the forum state.”

Offences under IT Act,2000 & ITA Act,2008:

Section 65 - Tampering with computer source documents

Section 66. Computer Related Offences. - If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment.....

66B Punishment for dishonestly receiving stolen computer resource or communication device.

66C Punishment for identity theft.

66D Punishment for cheating by personation by using computer resource.

66E Punishment for violation of privacy

66F Punishment for cyber terrorism.

67 Punishment for publishing or transmitting obscene material in electronic form.

67 A Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

67 C Preservation and retention of information by intermediaries.

71 Misrepresentation to the Controller or the Certifying Authority.

72 Offence relating to Breach of Confidentiality and Privacy

72A Offence relating to disclosure information in breach of lawful contract

73 Publishing Digital Signature Certificate false in certain particulars.

74 Offence relating to Publication of fraudulent purpose

84B Abetment of offence

84C Attempt to commit offences

Cyber Crimes against Property – Financial crimes – cheating on-line – illegal funds transfer

65. Tampering with Computer Source Documents.-

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to 2 lakh rupees, or with both.

Explanation - For the purposes of this section, "Computer Source Code" means the listing of programme, Computer Commands, Design and layout and program analysis of computer resource in any form.

Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh & Anr. in Cri. Petn. Nos. 2601 and 2602 of 2003 which has been decided by the Hon'ble High Court Of Andhra Pradesh on: 29.07.2005 and reported in 2005 CriLJ 4314

- 1. A cell phone is a computer as envisaged under the Information Technology Act.**
- 2. ESN and SID come within the definition of "computer source code" under section 65 of the Information Technology Act.**
- 3. When ESN is altered, the offence under Section 65 of Information Technology Act is attracted because every service provider has to maintain its own SID code and also give a customer specific number to each instrument used to avail the services provided.**
- 4. Whether a cell phone operator is maintaining computer source code, is a matter of evidence.**
- 5. In Section 65 of Information Technology Act the disjunctive word "or" is used in between the two phrases –**
 - a. "when the computer source code is required to be kept"**
 - b. "maintained by law for the time being in force"**

Cyber Law & Adjudication Issues in India:

Section 43. Penalty and Compensation for damage to computer, computer system, etc.

Section 46: Power to Adjudicate.

Section 47: Factors to be taken into account by the adjudicating officer.

Section 48: Establishment of Cyber Appellate Tribunal

**Hacking :
Resources
Trespassing**

**Hacking Laws:
Section 43 and 66
of IT Act**

**Civil Liabilities &
Criminal Offence**

43. Penalty and Compensation for damage to computer, computer system, etc. –
If any person without permission of the owner or any other person who is in charge of
a computer, computer system or computer network, -

- (a) Accesses or secures access to such computer, computer system or computer network or computer resource;**
- (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;**
- (c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;**
- (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network;**
- (e) Disrupts or causes disruption of any computer, computer system or computer network;**

- (f) Denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;**
- (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;**
- (h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;**
- (i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;**
- (j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;**

he shall be liable to pay damages by way of compensation to the person so affected.

43-A. Compensation for failure to protect data. –

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

45. Residuary Penalty.-

Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

61. Civil court not to have jurisdiction. -

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

Cyber Crimes against Nations – Cyber Terrorism – Damaging critical information infrastructures:

CYBERTERRORISM: Cyberterrorism is the convergence of terrorism and cyberspace.

Section 66F of ITA, 2008: Definition and Punishment of Cyberterrorism : Life Imprisonment.

Section 70 : Any person who secures access or attempts to secure access to a protected system punishable upto 10 years.

National Cyber Security Policy 2013 to protect "Critical Information Infrastructure" : 24 x 7 hours protection

On Line Defamation against Nation:

As we find in Krishnan vs. Krishnaveni, AIR, 1997 SC, 987, Section 499 of IPC is meant for defamation with respect to a person but it never includes defamation against the state or nation. Defamation against the state is covered under law of terrorism and if the process is through cyber world or online then it is terrorism.

Cyber Pornography : Child and Woman

1) Report of National Crime Records Bureau, 2013

Incidence Of Cases Registered And Number Of Persons Arrested Under Cyber Crimes (IT Act) During 2013 (All-India)

Offence: Obscene publication/transmission in electronic form : No. Of Case Registered: 1203 (28% of all cases under IT Act)

Person Arrested: 737 (35% of all cases under IT Act)

2) Report of National Crime Records Bureau, 2012

Incidence Of Cases Registered And Number Of Persons Arrested Under Cyber Crimes (IT Act) During 2012:

Offence: Obscene publication/transmission in electronic form : No. Of Case

Registered: 589 out of 2876 (20% of Total Cases under IT Act)(All India basis) In

West Bengal: No. Of Case Registered: 51 of 196 (26% of Total Cases under IT Act)

DPS MMS Case: In 2004 a young male school student of DPS had allegedly transmitted the clipping to few people containing picture of the girl who had participated in the sexual act which was captured in mobile phone.

The pictures spread throughout the country like fire through MMS and Email. It was a social death for the girl. It even spread across the world. The boy was arrested. A student of IIT Kharagpur had posted the said clipping on the auction web-site called 'baze.com' for sale. The student of IIT Kgp and the M.D. of 'baze.com' was arrested. Offence u/s 292 IPC and 67 IT, 2000 initiated.

Pornography

Hicklin' test of obscenity , : “I think the test of obscenity is this, whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall.

Miller Test: The *Millertest* was developed in the 1973 case *Miller vs.* It has three parts:

Whether "the average person, applying contemporary standards", would find that the work, taken as a whole, appeals to the prurient interest,

Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by applicable state law,

Whether the work, taken as a whole, lacks serious literary artistic political, or scientific value.

Justice Vijaya Kapse - Tahilramani of the Bombay High Court observed that simply viewing an obscene object is not an offence.

The Hon'ble Court quashed obscenity charges against top customs officers who were arrested following a police raid at a bungalow in Lonavla in 2008. The Hon'ble Court further observed that viewing an film in the privacy of a house is not obscenity as defined under Indian criminal law.

The accused were arrested on charges of allegedly watching a pornographic film on a laptop and dancing with bar girls, The Justice further observed if the obscene object is kept in a house for private viewing, the accused cannot be charged for obscenity. The court also observed that the private viewing of an obscene film on a laptop in a bungalow was not equivalent to public exhibition.

1) Satyam Sivam and Sundaram Case : FIR against Raj Kapur – Non Maintainable

2) In a recent judgment of this Court, Aveek Sarkar v. State of West Bengal, 2014 (4) SCC 257, this Court referred to English, U.S. and Canadian judgments and moved away from the Hicklin test and applied the contemporary community standards test.

Cyber Crimes against Obscenity etc.:

66-E. Punishment for violation of privacy.-

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation.- For the purposes of this section—

- (a) “Transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;**
- (b) “Capture”, with respect to an image, means to videotape, photograph, film or record by any means;**
- (c) “Private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;**

(d) “Publishes” means reproduction in the printed or electronic form and making it available for public;

(e) “Under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that-

(i) He or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or (ii) Any part of his or her private area

would not be visible to the public, regardless of whether that person is in a public or private place.

67. Punishment for publishing or transmitting obscene material in electronic form.-

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

67-A. Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form.-
Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

67-B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.-

Whoever,-

(a) Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct;

or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(d) Facilitates abusing children online; or

(e) Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that the provisions of section 67, section 67-A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) Which is kept or used for bonafide heritage or religious purposes.

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

Other Indian Laws That Deal With Pornography:

1)Indecent Representation Of Women (Prohibition) Act.

2) Indian Penal Code Section 293. Sale, Etc., Of Obscene Objects To Young Person 292. Sale, Etc., Of Obscene Books, Etc.

(3) The Protection Of Children From Sexual Offences Act, 2012:

"INTERMEDIARY": 2(W) OF ITA

- **"INTERMEDIARY" WITH RESPECT TO ANY PARTICULAR ELECTRONIC RECORD, MEANS ANY PERSON WHO ON BEHALF OF ANOTHER PERSON RECEIVES, STORES OR TRANSMITS THAT RECORD OR PROVIDES ANY SERVICE IN RESPECT TO THAT RECORD AND INCLUDES TELECOM SERVICE PROVIDERS, NETWORK SERVICE PROVIDERS, INTERNET SERVICE PROVIDERS, WEB-HOSTING SERVICE PROVIDERS, SEARCH ENGINES, ONLINE PAYMENT SITES, ONLINE AUCTION SITES, ONLINE MARKET PLACES AND CYBER CAFES.**

Role and Compliances by Intermediaries:

As per section 2(w) of the Information Technology Act as mended in 2008 the defined Intermediaries are as Follows

- 1) Internet Service Providers (ISP)**
- 2) Web Hosting provider and Blog Service providers**
- 3) Telecom Service Providers**
- 4) Network Service providers**
- 5) Search Engines**
- 6) Payment Service Provider/ Online Payment Service**
- 7) On Line Auction Sites**
- 8) Cyber Cafe.**
- 9) Social Network Service Providers**

Intermediary

Section 79 IT Act : Exemption from liability of intermediary in certain cases. --- Due Diligence

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him.

(2) The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(b) The intermediary does not-

(i) Initiate the transmission,

(ii) Select the receiver of the transmission, and

(iii) Select or modify the information contained in the transmission;

(c) The intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

3) The provisions of sub-section (1) shall not apply if-

(a) The intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act ;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

DUE DILIGENCE.....

- **DUE DILIGENCE IS A LEGAL DEFENCE TO A CHARGE CATEGORIZED AS STRICT LIABILITY. THE TERM MEANS THAT THE DEFENDANT TOOK REASONABLE ACTIONS TO AVOID THE OFFENCE FROM HAPPENING; HOWEVER, THROUGH NO FAULT OF THE DEFENDANT THE UNLAWFUL ACT TOOK PLACE NEVERTHELESS.**
- **THE DEFENCE IS REQUIRED TO PROVE THAT ALL REASONABLE CARE WAS TAKEN BY SHOWING EVIDENCE THAT THE JUDGE WILL WEIGH ON A BALANCE OF PROBABILITIES. THE PROSECUTION HOWEVER MUST PROVE THEIR CASE BY PROVING THAT THE PROHIBITED ACT WAS COMMITTED BEYOND A REASONABLE DOUBT. THE DEFENCE'S BURDEN IS FAR LESS RIDGED THAT THAT OF THE PROSECUTION.**

DUE DILIGENCE.....

- **WHEN ASSESSING THE DUE DILIGENCE EVIDENCE THE COURT IS DIRECTED TO ASK ITSELF “WHAT WOULD A REASONABLE PERSON DO IN LIKE CIRCUMSTANCES?” THIS IS KNOWN IN LAW AS THE TEST OF THE REASONABLE PERSON. IF THE DEFENDANT’S EVIDENCE FITS WITHIN THE GENERATE IMAGE OF THE REASONABLE PERSON THEN THE DEFENDANT WILL LIKELY BE SUCCESSFUL IN HIS/HER DEFENCE.**

DUE DILIGENCE(BLACK'S LAW DICTIONARY, 8TH ED. 2008)

- **DUE DILIGENCE IS A LEGAL DEFENCE TO A CHARGE CATEGORIZED AS STRICT LIABILITY. THE TERM MEANS THAT THE DEFENDANT TOOK REASONABLE ACTIONS TO AVOID THE OFFENCE FROM HAPPENING; HOWEVER, THROUGH NO FAULT OF THE DEFENDANT THE UNLAWFUL ACT TOOK PLACE NEVERTHELESS. BLACK'S LAW DICTIONARY DEFINES THE TERM AS "THE DILIGENCE REASONABLE EXPECTED FROM, AND ORDINARILY EXERCISED BY, A PERSON WHO SEEKS TO SATISFY A LEGAL REQUIREMENT OR TO DISCHARGE AN OBLIGATION."**

R. V. COURTAULDS FIBRES CANADA, [1992] O.J. NO. 1972

- **IN 1992 A HELPFUL DEFINITION OF THE DEFENCE OF DUE DILIGENCE WAS PRONOUNCED BY JUSTICE FITZPATRICK IN THE CASE OF R. V. COURTAULDS FIBRES CANADA. WHEREIN THE HONOURBLE COURT FOUND THAT “REASONABLE CARE AND DUE DILIGENCE DO NOT MEAN SUPERHUMAN EFFORTS. THEY MEAN A HIGH STANDARD OF AWARENESS AND DECISIVE, PROMPT, AND CONTINUING ACTION. TO DEMAND MORE, WOULD, IN MY VIEW, MOVE A STRICT LIABILITY OFFENCE DANGEROUSLY CLOSE TO ONE OF ABSOLUTE LIABILITY.”**

R. V. SAULT STE. MARIE [1978] S.C.J. NO. 59

- **IN 1978, IN THE CASE OF R. V. SAULT STE. MARIE, JUSTICE DICKSON RECOGNIZED THE AVAILABILITY OF THE DEFENCE OF DUE DILIGENCE WHERE THE OFFENCE WAS ONE OF STRICT LIABILITY. THIS MEANS THAT THE PROSECUTION NEED NOT PROVE THE INTENT OF THE DEFENDANT TO COMMIT THE OFFENCE, BUT ONLY THAT THE PROHIBITED ACT WAS COMMITTED. THE DEFENDANT CAN THEN CHOOSE TO AVOID LIABILITY BY SHOWING THAT ALL REASONABLE CARE WAS TAKEN.**

INFORMATION TECHNOLOGY (INTERMEDIARIES GUIDELINES) RULES, 2011.

- **2(D) "CYBER SECURITY INCIDENT" MEANS ANY REAL OR SUSPECTED ADVERSE EVENT IN RELATION TO CYBER SECURITY THAT VIOLATES AN EXPLICITLY OR IMPLICITLY APPLICABLE SECURITY POLICY RESULTING IN UNAUTHOTRISED ACCESS, DENIAL OF SERVICE OR DISRUPTION, UNAUTHORISED USE OF A COMPUTER RESOURCE FOR PROCESSING OR STORAGE OF INFORMATION OR CHANGES TO DATA, INFORMATION WITHOUT AUTHORISATION;**
- **J) "USER" MEANS ANY PERSON WHO ACCESS OR AVAIL ANY COMPUTER RESOURCE OF INTERMEDIARY FOR THE PURPOSE OF HOSTING, PUBLISHING, SHARING, TRANSACTING, DISPLAYING OR UPLOADING INFORMATION OR VIEWS AND INCLUDES OTHER PERSONS JOINTLY PARTICIPATING IN USING THE COMPUTER RESOURCE OF AN INTERMEDIARY.**

RULE 3. DUE DILIGENCE TO BE OBSERVED BY INTERMEDIARY

- **THE INTERMEDIARY SHALL OBSERVE FOLLOWING DUE DILIGENCE WHILE DISCHARGING HIS DUTIES, NAMELY :—**
- **(1) THE INTERMEDIARY SHALL PUBLISH THE RULES AND REGULATIONS, PRIVACY POLICY AND USER AGREEMENT FOR ACCESS-OR USAGE OF THE INTERMEDIARY'S COMPUTER RESOURCE BY ANY PERSON.**
- **(2) SUCH RULES AND REGULATIONS, TERMS AND CONDITIONS OR USER AGREEMENT SHALL INFORM THE USERS OF COMPUTER RESOURCE NOT TO HOST, DISPLAY, UPLOAD, MODIFY, PUBLISH, TRANSMIT, UPDATE OR SHARE ANY INFORMATION THAT —**
- **A) BELONGS TO ANOTHER PERSON AND TO WHICH THE USER DOES NOT HAVE ANY RIGHT TO; B) IS GROSSLY HARMFUL, HARASSING, BLASPHEMOUS DEFAMATORY, OBSCENE, PORNOGRAPHIC, PAEDOPHILIC, LIBELLOUS, INVASIVE OF ANOTHER'S PRIVACY, HATEFUL, OR RACIALLY, ETHNICALLY OBJECTIONABLE, DISPARAGING, RELATING OR ENCOURAGING MONEY LAUNDERING OR GAMBLING, OR OTHERWISE UNLAWFUL IN ANY MANNER WHATEVER;**
- **C) HARM MINORS IN ANY WAY;**

- **D) INFRINGES ANY PATENT, TRADEMARK, COPYRIGHT OR OTHER PROPRIETARY RIGHTS;**
- **(E) VIOLATES ANY LAW FOR THE TIME BEING IN FORCE; E) DECEIVES OR MISLEADS THE ADDRESSEE ABOUT THE ORIGIN OF SUCH MESSAGES OR COMMUNICATES ANY INFORMATION WHICH IS GROSSLY OFFENSIVE OR MENACING IN NATURE; F) IMPERSONATE ANOTHER PERSON;**
- **H) CONTAINS SOFTWARE VIRUSES OR ANY OTHER COMPUTER CODE, FILES OR PROGRAMS DESIGNED TO INTERRUPT, DESTROY OR LIMIT THE FUNCTIONALITY OF ANY COMPUTER RESOURCE;**
- **I) THREATENS THE UNITY, INTEGRITY, DEFENCE, SECURITY OR SOVEREIGNTY OF INDIA, FRIENDLY RELATIONS WITH FOREIGN STATES, OR PUBLIC ORDER OR CAUSES INCITEMENT TO THE COMMISSION OF ANY COGNISABLE OFFENCE OR PREVENTS INVESTIGATION OF ANY OFFENCE OR IS INSULTING ANY OTHER NATION**

- **(3) THE INTERMEDIARY SHALL NOT KNOWINGLY HOST OR PUBLISH ANY INFORMATION OR SHALL NOT INITIATE THE TRANSMISSION, SELECT THE RECEIVER OF TRANSMISSION, AND SELECT OR MODIFY THE INFORMATION CONTAINED IN THE TRANSMISSION AS SPECIFIED IN SUB-RULE (2): PROVIDED THAT THE FOLLOWING ACTIONS BY AN INTERMEDIARY SHALL NOT AMOUNT TO HOSTING, PUBLISHING, EDITING OR STORING OF ANY SUCH INFORMATION AS SPECIFIED IN SUB-RULE: (2)**
 - (A) TEMPORARY OR TRANSIENT OR INTERMEDIATE STORAGE OF INFORMATION AUTOMATICALLY WITHIN THE COMPUTER RESOURCE AS AN INTRINSIC FEATURE OF SUCH COMPUTER RESOURCE, INVOLVING NO EXERCISE OF ANY HUMAN EDITORIAL CONTROL, FOR ONWARD TRANSMISSION OR COMMUNICATION TO ANOTHER COMPUTER RESOURCE; (B) REMOVAL OF ACCESS TO ANY INFORMATION, DATA OR COMMUNICATION LINK BY AN INTERMEDIARY AFTER SUCH INFORMATION, DATA OR COMMUNICATION LINK COMES TO THE ACTUAL KNOWLEDGE OF A PERSON AUTHORISED BY THE INTERMEDIARY PURSUANT TO ANY ORDER OR DIRECTION AS PER THE PROVISIONS OF THE ACT;**

(4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes,

(5) The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the Intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove non- compliant information..

(6) The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.

(7) When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.

- **(8) THE INTERMEDIARY SHALL TAKE ALL REASONABLE MEASURES TO SECURE ITS COMPUTER RESOURCE AND INFORMATION CONTAINED THEREIN FOLLOWING THE REASONABLE SECURITY PRACTICES AND PROCEDURES AS PRESCRIBED IN THE INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL INFORMATION) RULES, 2011.**
- **(9) THE INTERMEDIARY SHALL REPORT CYBER SECURITY INCIDENTS AND ALSO SHARE CYBER SECURITY INCIDENTS RELATED INFORMATION WITH THE INDIAN COMPUTER EMERGENCY RESPONSE TEAM. (**

(10) The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to "perform thereby circumventing any law for the time being in force: provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.

(11) The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule 3 can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

INTERMEDIARIES NOT LIABLE IN CERTAIN CASES:

Unless otherwise specifically provided to the contrary, an intermediary will be not liable for, any third party information, data or communication link made by him. This exemption is available only if:

- The intermediary's role is limited to providing access to a communication system over which third parties transmit information or temporarily store the same.**

- The intermediary does not**

- 1.Initiate the transmission**

- 2.Select the receiver of transmission or,**

- 3.Modify the information contained in the transmission.**

The exemption would however stand withdrawn if intermediary conspires or abets the commission of an unlawful act or after having received the information from the government that any information, data or communication link residing in or connected with computer resources controlled by the intermediary, are being used to commit unlawful acts and such intermediary fails to act expeditiously in removing or disabling access to such link or resource.

Sanjay Kumar Kedia vs Narcotics Control Bureau & Anr on 3 December, 2007, Bench: S.B.Sinha, Harjit Singh Bedi, Supreme Court of India, Appeal (crl.) 1659 of 2007, DATE OF JUDGMENT: 03/12/2007, BENCH: S.B.SINHA & HARJIT SINGH BEDI:

Truevalueprescriptions.com: Review of this website indicated that this website was a internet pharmacy.....as a drug available for sale..... orders for drugs could be made without a prescription from the TRUEVALUE website..... orders for drugs could be placed without seeing a doctor. DEA, conducted a "whois" reverse look-up on domain name TRUEVALUEPRESCRIPTIONS.COM at domaintools.com and revealed that IP address was 203.86.100.76 and the server that hosts the website was located at Palcom, Delhi which also belongs to Xponse.....were not acting merely as a network service provider but were actually running internet pharmacy and dealing withthe appellant and his associates were not innocent intermediaries or network service providers as defined under **section 79 of the Technology Act but the said business was only a fagade and camouflage for more sinister activity. In this situation, **Section 79** will not grant immunity to an accused who has violated the provisions of the Act as this provision gives immunity from prosecution for an offence only under **Technology Act** itself.**

SECTION 72A IN THE INFORMATION TECHNOLOGY ACT, 2000

- **72A PUNISHMENT FOR DISCLOSURE OF INFORMATION IN BREACH OF LAWFUL CONTRACT. -SAVE AS OTHERWISE PROVIDED IN THIS ACT OR ANY OTHER LAW FOR THE TIME BEING IN FORCE, ANY PERSON INCLUDING AN INTERMEDIARY WHO, WHILE PROVIDING SERVICES UNDER THE TERMS OF LAWFUL CONTRACT, HAS SECURED ACCESS TO ANY MATERIAL CONTAINING PERSONAL INFORMATION ABOUT ANOTHER PERSON, WITH THE INTENT TO CAUSE OR KNOWING THAT HE IS LIKELY TO CAUSE WRONGFUL LOSS OR WRONGFUL GAIN DISCLOSES, WITHOUT THE CONSENT OF THE PERSON CONCERNED, OR IN BREACH OF A LAWFUL CONTRACT, SUCH MATERIAL TO ANY OTHER PERSON, SHALL BE PUNISHED WITH IMPRISONMENT FOR A TERM WHICH MAY EXTEND TO THREE YEARS, OR WITH FINE WHICH MAY EXTEND TO FIVE LAKH RUPEES, OR WITH BOTH.**

69 Power to issue directions for interception or monitoring or decryption of any information through any computer resource. =

(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to-

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.]

69A Power to issue directions for blocking for public access of any information through any computer resource. =

(1) Where the Central Government or any of its officer specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2) for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARDS FOR BLOCKING FOR ACCESS OF INFORMATION BY PUBLIC) RULES, 2009.

- **5. DIRECTION BY DESIGNATED OFFICER.--**
- **THE DESIGNATED OFFICER MAY, ON RECEIPT OF ANY REQUEST FROM THE NODAL OFFICER OF AN ORGANISATION OR A COMPETENT COURT, BY ORDER DIRECT ANY AGENCY OF THE GOVERNMENT OR INTERMEDIARY TO BLOCK FOR ACCESS BY THE PUBLIC ANY INFORMATION OR PART THEREOF GENERATED, TRANSMITTED, RECEIVED, STORED OR HOSTED IN ANY COMPUTER RESOURCE FOR ANY OF THE REASONS SPECIFIED IN SUB-SECTION (1) OF SECTION 69A OF THE ACT.**
- **9. BLOCKING OF INFORMATION IN CASES OF EMERGENCY:**
- **12. ACTION FOR NON-COMPLIANCE OF DIRECTION BY INTERMEDIARY.--**
- **IN CASE THE INTERMEDIARY FAILS TO COMPLY WITH THE DIRECTION ISSUED TO HIM UNDER RULE 9, THE DESIGNATED OFFICER SHALL, WITH THE PRIOR APPROVAL OF THE SECRETARY, DEPARTMENT OF INFORMATION TECHNOLOGY, INITIATE APPROPRIATE ACTION AS MAY BE REQUIRED TO COMPLY WITH THE PROVISIONS OF SUB-SECTION (3) OF SECTION 69A OF THE ACT.**

- **13. INTERMEDIARY TO DESIGNATE ONE PERSON TO RECEIVE AND HANDLE DIRECTIONS.--**
- **(1) EVERY INTERMEDIARY SHALL DESIGNATE AT FEAST ONE PERSON TO RECEIVE AND HANDLE THE DIRECTIONS FOR BLOCKING OF ACCESS BY THE PUBLIC ANY INFORMATION GENERATED, TRANSMITTED, RECEIVED, STORED OR HOSTED IN ANY COMPUTER RESOURCE UNDER THESE RULES.**
- **(2) THE DESIGNATED PERSON OF THE INTERMEDIARY SHALL ACKNOWLEDGE RECEIPT OF THE DIRECTIONS TO THE DESIGNATED OFFICER WITHIN TWO HOURS ON RECEIPT OF THE DIRECTION THROUGH ACKNOWLEDGEMENT LETTER OR FAX OR E-MAIL SIGNED WITH ELECTRONIC SIGNATURE.**

69B. Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security.- (1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section,

(i) "Computer Contaminant" shall have the meaning assigned to it in section 43

(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARD FOR MONITORING AND COLLECTING TRAFFIC DATA OR INFORMATION) RULES, 2009.

- **(F) “CYBER SECURITY INCIDENT” MEANS ANY REAL OR SUSPECTED ADVERSE EVENT IN RELATION TO CYBER SECURITY THAT VIOLATES AN EXPLICITLY OR IMPLICITLY APPLICABLE SECURITY POLICY RESULTING IN UNAUTHORISED ACCESS, DENIAL OF SERVICE/DISRUPTION, UNAUTHORISED USE OF A COMPUTER RESOURCE FOR PROCESSING OR STORAGE OF INFORMATION OR CHANGES TO DATA, INFORMATION WITHOUT AUTHORISATION;**
- **(G) “CYBER SECURITY BREACHES” MEANS UNAUTHORISED ACQUISITION OR UNAUTHORISED USE BY A PERSON OF DATA OR INFORMATION THAT COMPROMISES THE CONFIDENTIALITY, INTEGRITY OR AVAILABILITY OF INFORMATION MAINTAINED IN A COMPUTER RESOURCE**

5. Intermediary to ensure effective check in handling monitoring or collection of traffic data or information.— The intermediary or person in-charge of computer resources shall put in place adequate and effective internal checks to ensure that unauthorised monitoring or collection of traffic data or information does not take place and extreme secrecy is maintained and utmost care and precaution is taken in the matter of monitoring or collection of traffic data or information as it affects privacy of citizens and also that this matter is handled only by the designated officer of the intermediary or person in-charge of computer resource.

6. Responsibility of intermediary.— The intermediary or person in-charge of computer resource shall be responsible for the actions of their employees also, and in case of violation of the provision of the Act and rules made thereunder pertaining to maintenance of secrecy and confidentiality of information or any unauthorised monitoring or collection of traffic data or information, the intermediary or person in-charge of computer resource shall be liable for any action under the relevant provision of the laws for the time being in force.

9. Prohibition of monitoring or collection of traffic data or information without authorisation.—

(1) Any person who, intentionally or knowingly, without authorisation under sub-rule (2) of rule 3 or sub-rule (1) of rule 4, monitors or collects traffic data or information, or attempts to monitor or collect traffic data or information, or authorises or assists any person to monitor or collect traffic data or information in the course of its occurrence or transmission at any place within India, shall be proceeded against, punished accordingly under the relevant provisions of the law for the time being in force.....

10. Prohibition of disclosure of traffic data or information by authorised agency.— The details of monitored or collected traffic data or information shall not be used or disclosed by the agency authorised under sub-rule (1) of rule 4 for any other purpose, except for forecasting imminent cyber threats or general trend of port-wise traffic on Internet, or general analysis of cyber incidents, or for investigation or in judicial proceedings before the competent court in India.

11. Maintenance of confidentiality.— Save as otherwise provided in rule 10, strict confidentiality shall be maintained in respect of directions for monitoring or collection of traffic data or information issued by the competent authority under these rules.

76. Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

77. Compensation, penalties or confiscation not to interfere with other punishment.- No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

77-A. Compounding of Offences.-

(1) A 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 this Act.

Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.

Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(2) The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265-B and 265-C of Code of Criminal Procedures, 1973 shall apply.

77-B. Offences with three years imprisonment to be cognizable.-

(1) Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

78. Power to investigate offences.-

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act.

Section 80 of the IT Act

- i. Inspector or any person authorized by Govt.**
- ii. Enter any public place, search and arrest without warrant allowed**
- iii. Committed, committing and about to commit offence under this Act**
- iv. Public places includes public conveyance, any hotel, any shop and any place intended for use by, or accessible to the public.**
- v. Arrest by other than police officer to be taken to nearest Court or P.S.**
- vi. Subject to IT Act, Provisions of Cr.P.C. will be applicable.**

81-A. Application of the Act to Electronic cheque and Truncated cheque. -

(1) The provisions of this Act, for the time being in force, shall apply to, or in relation to, electronic cheques and the truncated cheques subject to such modifications and amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 (26 of 1881) by the Central Government, in consultation with the Reserve Bank of India, by notification in the Official Gazette.

81. Act to have Overriding effect.-

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act, 1970 (39 of 1970).

84-A. Modes or methods for encryption. –

The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption.

84-C. Punishment for attempt to commit offences.

Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

84-B. Punishment for abetment of offences.

Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation: An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

85. Offences by Companies.-

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly: Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

70. Protected system.-

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation: For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system.

Power of the other authorities

Section 70-A: National nodal agency.

Section 70-B: Indian Computer Emergency Response Team to serve as national agency for incident response.

CERT-In : CERT-In is formed to look into cyber attacks affecting I-T dept of banks etc.

88. Constitution of Advisory Committee.

Section 5 of Indian Telegraph Act

5 (2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order:

Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section.

Lawful Interception of Voice and Data in the Investigation of Crimes - Legal Procedures:

1) Relevant Information Technology Act with Amendment Act

2) Rules under IT Act

69. Powers to issue directions for interception or monitoring or decryption of any information through any computer resource.-

69-A. Power to issue directions for blocking for public access of any information through any computer resource.-

69-B. Power to authorise to monitor and collect traffic data or information through any computer resource for Cyber Security.

Information Technology (Directions for Interception or Monitoring or Decryption of Information) Rules, 2009 Spells out the procedure for taping of electronic communications under the IT Act.

Maharashtra v. Bharat Shanti Lal Shah & others

In State of Maharashtra v. Bharat Shanti Lal Shah & others ((2008) 13 SCC 5) the Hon'ble Court observed "The interpretation of conversation though constitutes an invasion of an individual right to privacy but the said right can be curtailed in accordance with procedure validly established by law. Thus what the Court is required to see is that the procedure itself must be fair, just and reasonable and non-arbitrary, fanciful or oppressive."

Relevant part of Land Mark Judgement on Evidentiary Value of intercepted data: Dharambir Khattar vs Union Of India & Another on 21 November, 2012 by Hon'ble High Court Of Delhi.

“Therefore, without going into the issue of whether there was non-compliance of the provisions of Section 5(2) or of Rule 419-A, it is clear that even if there was, in fact, no compliance, the evidence gathered thereupon would still be admissible. This is the clear position settled by the Supreme Court and, therefore, no further question of law arises on this aspect of the matter.”

Rule 419A of the Indian Telegraph Rules, 1951::

The Central Government made the following rules to amend the Indian Telegraph Rules, 1951:

G.S.R. 193 (E).— In exercise of the powers conferred by Section 7 of the Indian Telegraph Act, 1885 (13 of 1885), the Central Government hereby makes the following rules further to amend the Indian Telegraph Rules, 1951, namely:—

- 1. (1) These rules may be called the Indian Telegraph (Amendment) Rules, 2007.**
- (2) They shall come into force on the date of their publication in the Official Gazette.**
- 2. In the Indian Telegraph Rules, 1951, after rule 419, the following rule shall be substituted, namely:—**

“419-A. (1) Directions for interception of any message or class of messages under sub-section (2) of Section 5 of the Indian Telegraph Act, 1885 (hereinafter referred to as the said (Act) shall not be issued except by an order made by the Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India and by the Secretary to the State Government in-charge of the Home Department in the case of a State Government. In unavoidable circumstances, such order may be made by an officer, not below the rank of a Joint Secretary to the Government of India, who has been duly authorized by the Union Home Secretary or the State Home Secretary, as the case may be:

Provided that in emergent cases—

(i) in remote areas, where obtaining of prior directions for interception of messages or class of messages is not feasible; or

(ii) for operational reasons, where obtaining of prior directions for interception of message or class of messages is not feasible;

the required interception of any message or class of messages shall be carried out with the prior approval of the Head or the second senior most officer of the authorized security i.e. Law Enforcement Agency at the Central Level and the officers authorised in this behalf, not below the rank of Inspector General of Police at the state level but the concerned competent authority shall be informed of such interceptions by the approving authority within three working days and that such interceptions shall be got confirmed by the concerned competent authority within a period of seven working days. If the confirmation from the competent authority is not received within the stipulated seven days, such interception shall cease and the same message or class of messages shall not be intercepted thereafter without the prior approval of the Union Home Secretary or the State Home Secretary, as the case may be.

(2) Any order issued by the competent authority under sub-rule (1) shall contain reasons for such direction and a copy of such order shall be forwarded to the concerned Review Committee within a period of seven working days.

(3) While issuing directions under sub-rule (1) the officer shall consider possibility of acquiring the necessary information by other means and the directions under sub-rule (1) shall be issued only when it is not possible to acquire the information by any other reasonable means.

(4) The interception directed shall be the interception of any message or class of messages as are sent to or from any person or class of persons or relating to any particular subject whether such message or class of messages are received with one or more addresses, specified in the order, being an address or addresses likely to be used for the transmission of communications from or to one particular person specified or described in the order or one particular set of premises specified or described in the order.

(5) The directions shall specify the name and designation of the officer or the authority to whom the intercepted message or class of messages is to be disclosed and also specify that the use of intercepted message or class of messages shall be subject to the provisions of sub-section (2) of Section 5 of the said Act.

(6) The directions for interception shall remain in force, unless revoked earlier, for a period not exceeding sixty days from the date of issue and may be renewed but the same shall not remain in force beyond a total period of one hundred and eighty days.

(7) The directions for interception issued under sub-rule (1) shall be conveyed to the designated officers of the service provider(s) who have been granted licenses under Section 4 of the said Act, in writing or by secure electronic communication by an officer not below the rank of Superintendent of Police or the officer of the equivalent rank and mode of secure electronic communication and its implementation shall be as determined by the telegraph authority.

(8) The officer authorized to intercept any message or class of message shall maintain proper records mentioning therein, the intercepted message or class of messages, the particulars of persons whose message has been intercepted, the name and other particulars of the officer or the authority to whom the intercepted message or class of messages has been disclosed, the number of copies of the intercepted message or class of messages made and the mode or the method by which such copies are made, the date of destruction of the copies and the duration within which the directions remain in force.

(9) All the requisitioning Security and Law Enforcement Agencies shall designate one or more nodal officers not below the rank of Superintendent of Police or the officer of the equivalent rank to authenticate and send the requisitions for interception to the designated officers of the telegraph authority or the concerned service providers, as the case may be and the delivery of written requisition for interception shall be done by an officer not below the rank of Sub-inspector of Police.

(10) The telegraph authority shall designate officer(s) in every licensed service area/State/Union Territory as the nodal officers to receive and handle such requisitions for interception and the service providers shall designate two senior officer(s) of the company in every licensed service area/State/Union Territory as the nodal officers to receive and handle such requisitions for interception.

(11) The designated nodal officer(s) of the telegraph authority or the service providers shall issue acknowledgment to the requisitioning Security and Law Enforcement Agency within two hours on receipt of intimations for interception.

(12) The system of designated nodal officers for communicating and receiving the requisitions for interceptions shall also be followed in emergent cases/unavoidable cases where prior approval of the competent authority has not been obtained.

(13) The designated nodal officers of the telegraph authority or the service providers shall forward every fifteen days a list of interception authorizations received by them during the preceding fortnight to the nodal officers of the Security and Law Enforcement Agencies for confirmation of the authenticity of such authorizations and the list shall include details such as the reference and date of orders of the Union Home Secretary or State Home Secretary, or orders issued by officer other than competent authority, in terms of sub-rule (1) in emergent cases which were not subsequently confirmed by the competent authority, date and time of receipt of such orders and the date and time of Implementation of such orders.

(14) The service providers shall put in place adequate and effective internal checks to ensure that unauthorized interception of messages does not take place and extreme secrecy is maintained and utmost care and precaution is taken in the matter of interception of messages as it affects privacy of citizens and also that this matter is handled only by the designated nodal officers of the company.

(15) The service providers shall be responsible for actions of their employees also and in case of established violation of license conditions pertaining to maintenance of secrecy and confidentiality of information and unauthorized interception of communication, action shall be taken against the service providers as per Provisions of the said Act and this shall include not only fine but also suspension or revocation of their licenses.

(16) The Central Government and the State Government, as the case may be, shall constitute a Review Committee.

(17) The Review Committee shall meet at least once in two months and record its findings whether the directions issued under sub-rule (1) are in accordance with the provisions of sub-section (2) of Section 5 of the said Act and when the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above it may set aside the directions and orders for destruction of the copies of the intercepted message or class of messages.

(18) Records pertaining to such directions for interception and of intercepted messages shall be destroyed by the relevant competent authority and the authorized Security and Law Enforcement Agencies every six months unless these are, or likely to be, required for functional requirements.

(19) The service providers and telegraph authority shall destroy records pertaining to directions for interception of messages within two months of discontinuance of the interception of such messages and in doing so they shall maintain extreme secrecy”.

**SUBPOENA REQUEST
PRESERVATION LETTER
EMERGENCY DISCLOSURE**

Subpoena is a writ issued by a government agency, most often a court, to compel testimony by a witness or production of evidence under a penalty for failure. Subpoena may be of two types and they are:

***Subpoena ad testificandum:* It orders a person to testify before the ordering authority or face punishment.**

***Subpoena duces tecum:* It orders a person or organization to bring physical evidence before the ordering authority or face punishment. This is often used for requests to mail copies of documents to the requesting party or directly to court.**

***Sub poena* meaning "under penalty".**

<https://en.wikipedia.org/wiki/Subpoena>

United States District Court

Anne Anderson, et al.
v.
W.R. Grace & Co., et al.

DISTRICT Massachusetts
DOCKET NO. 82-1672-S
TYPE OF CASE ☒ CIVIL ☐ CRIMINAL
SUBPOENA FOR ☒ PERSON ☒ DOCUMENT(S) or OBJECT

TO:

Keeper of the Records
United States Geological Survey
151 Causeway Street, Suite 1001
Boston, Massachusetts 02114-1384

YOU ARE HEREBY COMMANDED to appear in the United States District Court at the place, date, and time specified below to testify in the above-entitled case.

PLACE United States District Court J. W. McCormack Post Office and Courthouse Boston, Massachusetts	COURTROOM <u>6, 15th floor</u> DATE AND TIME ** <u>Monday</u> <u>June 16, 19</u> <u>9:00 a.m.</u>
--	--

YOU ARE ALSO COMMANDED to bring with you the following document(s) or object(s):⁽¹⁾

SEE ATTACHED SCHEDULE

ATTEST: A TRUE COPY

David M. Greal
CONSTABLE



☐ See additional information on reverse

This subpoena shall remain in effect until you are ordered to depart by the court or by an officer acting on behalf of the court.

U.S. MAGISTRATE(S) OR CLERK OF COURT
GEORGE P. McGRATH

DATE
June 11, 19

(BY) DEPUTY CLERK

Charles Lyons

This subpoena is issued upon application of the:

☐ Plaintiff ☒ Defendant ☐ U.S. Attorney

ATTORNEY'S NAME AND ADDRESS
Carl M. Perkins
Foley, Hoag & Eliot
One Post Office Square
Boston, MA 02109 (617) 482-1390

⁽¹⁾ If not applicable, enter "none."

⁽²⁾ A subpoena shall be issued by a magistrate in a proceeding before him, but need not be under the seal of the court. (Rule 17(c), Federal Rules of Criminal Procedure.)

** You may not be needed on the date indicated; please call Carl Perkins Erin O'Brien (at 617-482-1390) to discuss scheduling.

Section 174 in The Indian Penal Code:

174. Non-attendance in obedience to an order from public servant.—Whoever, being legally bound to attend in person or by an agent at a certain place and time in obedience to a summons, notice, order or proclamation proceeding from any public servant legally competent, as such public servant, to issue the same, intentionally omits to attend at that place or time, or departs from the place where he is bound to attend before the time at which it is lawful for him to depart, shall be punished with simple imprisonment for a term which may extend to one month, or with fine which may extend to five hundred rupees, or with both, or, if the summons, notice, order or proclamation is to attend in person or by agent in a Court of Justice, with simple imprisonment for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both. Illustrations

(a) A, being legally bound to appear before the 1[High Court] at Calcutta, in obedience to a subpoena issuing from that Court, intentionally omits to appear. A has committed the offence defined in this section.

(b) A, being legally bound to appear before a ¹⁷⁶ [District Judge], as a witness, in obedience to a summons issued by that 2[District Judge] intentionally omits to appear. A has committed the offence defined in this section.

Preservation Letter:

ØThe goal of the preservation letter is, of course, to remind opponents to preserve evidence, to be sure the evidence doesn't disappear.

ØWhen evidence is a paper document, preserving it is simple.

ØBy contrast, preserving electronic data poses unique challenges because: □

ØTouching data changes it □

ØDigital evidence is increasingly ill-suited to printing □

ØData must be interpreted to be used Storage media are fragile and changing all the time □

ØDigital storage media are dynamic and recyclable.

The ways that information's destroyed on personal computer:

1. Completely overwriting the deleted data on magnetic media (e.g., floppy disks, tapes or hard drives) with new information;

2. Strongly encrypting the data and then “losing” the encryption key; or,

3. Physically damaging the media to such an extent that it cannot be read.

Sample Preservation Letter:

RE: [MATTER]

Dear _____

Please be advised that Electronically Stored Information (“ESI”) has been determined to be relevant in this matter and you are being given notice that you are hereby required to preserve such ESI as described herein. This preservation notice and the description of potentially relevant ESI shall in no way constitute the entirety of the ESI you are obligated to preserve, but a minimum requirement based on CLIENT’S current understanding of your computer systems as well as computer systems in general.

These computer systems may be owned or maintained by you, your employees, third parties or contractors. Any ESI you deem potentially relevant in addition to any noted herein shall be preserved.

Electronically Stored Files – You are required to preserve:

- **Active data**

Archive data (backups, local or otherwise).

- **Deleted data (data deleted by a user or a system process but still recoverable through forensic methods).**
- **Media used to house active data and media used to house backup data as well as any hardware specifically required to access the media (hard disk drives, tape drives, magneto-optical drives, etc).**
- **Cloud/Internet data stored on remote servers, computers or other storage devices.....**

PRESERVATION REQUIREMENTS

You are required to preserve the above items as they include or pertain to:

- **Specific, relevant persons or groups, including, but not limited to: (Names, Groups, Parties)**
- **Specific, relevant topics or keywords, including, but not limited to: (Topics, Keywords)**
- **Specific, relevant time frames or dates, including, but not limited to: (Date Ranges)**

67-C. Preservation and Retention of information by intermediaries.-

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Emergency Disclosure Request:

What kinds of emergency cases?

Sometimes we voluntarily disclose user information to government agencies when we believe that doing so is necessary to prevent death or serious physical harm to someone. The law allows us to make these exceptions, such as in cases involving kidnapping or bomb threats. Emergency requests must contain a description of the emergency and an explanation of how the information requested might prevent the harm. Any information we provide in response to the request is limited to what we believe would help prevent the harm.

https://www.google.com/transparencyreport/userdatarequests/legalprocess/#what_kinds_of_emergency

Providers can disclose information to government entities if:

“.... The provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.”

- 18 U.S.C. Sec. 2702 (b) (8)]

Section 166A in The Code Of Criminal Procedure, 1973

166A. ² Letter of request competent authority for investigation in a country or place outside India.

(1) Notwithstanding anything contained in this Code, if, in the course of an investigation into an offence, an application is made by the investigating officer or any officer superior in rank to the investigating officer that evidence may be available in a country or place outside India, any Criminal Court may issue a letter of request to a Court or an authority in that country or place competent to deal with such request to examine orally any person supposed to be acquainted with the facts and circumstances of the case and to record his statement made in the course of such examination and also to require such person or any other person to produce any document or thing which may be in his possession pertaining to the case and to forward all the evidence so taken or collected or the authenticated copies thereof or the thing so collected to the Court issuing such letter.

(2) The letter of request shall be transmitted in such manner as the Central Government may specify in this behalf.

(3) Every statement recorded or document or thing received under sub- section (1) shall be deemed to be the evidence collected during the course of investigation under this Chapter.

CrPC 166B: Section 166B of the Criminal Procedure Code

Letter of request from a country or place outside India to a Court or an authority for investigation in India

Upon receipt of a letter of request from a Court or an authority in a country or place outside India competent to issue such letter in that country or place for the examination of any person or production of any document or thing in relation to an offence under investigation in that country or place, the Central Government may, if it thinks fit-

**forward the same to the Chief Metropolitan Magistrate or Chief Judicial Magistrate or such Metropolitan Magistrate or Judicial Magistrate as he may appoint in this behalf, who shall thereupon summon the person before him and record his statement or cause the document or thing to be produced, or
send the letter to any police officer for investigation, who shall thereupon investigate into the offence in the same manner, as if the offence had been committed within India.**

All the evidence taken or collected under Sub-Section (1), or authenticated copies thereof or the thing so collected, shall be forwarded by the Magistrate or police officer, as the case may be, to the Central Government for transmission to the Court or the authority issuing the letter of request, in such manner as the Central Government may deem fit.

Cloud Computing & Mobile Phone

Cloud computing is the latest buzz in Information Technology ecosystem. It entrusts remote services with user's data, software and computation. In the present time more Smart Phones, Tablets, I-Pads are getting connected to cloud computing as it provides huge benefits in accessing remote resources. But Cloud Computing has associated with a lot of risks and apprehension of lack of security.

Mobile phone has the same evidentiary value as other digital media and has great similarities with computer. The Source of evidence for mobile phone are 1) Media Devices, 2) SIM card, 3) Memory Chips, 4) Network providers.

Evidence in Cloud

**Cloud service delivery models:
Infrastructure as a Service (IaaS),
Platform as a Service (PaaS), and
Software as a Service (SaaS).**

The protection of clients is effectuated through the case of *Banyan Tree Holding (P.) Ltd. V. A. Murali Krishnan Reddy & Anr*, 2010 (42) PTC 361 (Del), that has clarified the law on this point by elucidating the following principles :

- 1) Mere accessibility of the foreign website in a particular area would not enable the Court to exercise jurisdiction.**
- 2) A passive website, with no intention to specifically target audiences outside the State where the host of the website is located, cannot vest the forum court with Jurisdiction.**
- 3) The website in question must be an interactive one which provides opportunity of engaging with customers in the area where jurisdiction is sought.**

**84. Protection of Action taken in Good Faith.-
No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Chairperson, Members, Adjudicating Officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made there under.**

CHAIN OF CUSTODY AND LIVE CYCLE OF DIGITAL EVIDENCE:

Chain of custody may be defined as “A road map that shows how evidence was collected, analyzed, and preserved in order to be presented as evidence in court”. (John Vacca, P-154) [1] . Chain of custody plays a very important role in digital investigation process. This is a phrase that refers to the accurate auditing and control of original evidence material that could potentially be used for legal purpose.

Investigator must know how to answer certain questions in the whole forensic investigation process:

- 1. What is digital evidence?**
- 2. Where was digital evidence discovered, collected, handled and/or examined?**
- 3. Who came into contact with digital evidence, handled it, and discovered it?**
- 4. What's the reason for using the digital evidence?**
- 5. When the digital evidence is discovered, accessed, examined or transferred?**
- 6. How is digital evidence used?**

Welcoming Electronic Records/Evidence

Section 3. Authentication of Electronic Records

Section 3-A. Electronic Signature Authentication

Section 4 of IT Act: Legal Recognition of Electronic Records.

Section 5. Legal recognition of Electronic Signature.

Section 10-A. Validity of contracts formed through electronic means.

4. Legal Recognition of Electronic Records. -

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -

(a) Rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

The mobile call records reveal only first 14 digit out of 15 digit and the last digit is always missing which is known as “Check Digit”

“ One more point has to be clarified. In the seizure memo (Ext. 61/4), the IMEI number of Nokia phone found in the truck was noted as ...52432. That means the last digit '2' varies from the call records wherein it was noted as ...52430. Thus, there is a seeming discrepancy as far as the last digit is concerned. This discrepancy stands explained by the evidence of PW 78 – a computer Engineer working as Manager, Siemens. He stated, while giving various details of the 15 digits, that the last one digit is a spare digit and the last digit, according to GSM specification should be transmitted by the mobile phone as '0'...”: State (NCT of Delhi) v. Navjot Sandhu, AIR2005SC3820 , The Hon'ble Supreme Court.

Recent Conviction in West Bengal.

Nature of Electronic Evidence

Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device

Electronic evidence is, by its very nature, fragile.

It can be altered, damaged, or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence.

The nature of electronic evidence is such that it poses special challenges for its admissibility in court.

Chain-of-custody is the collection, preservation and analysis of evidence for the purpose of establishing authenticity and reliability of evidence.

Evidentiary value of E-mail:

Apart from the importance of the mode of proving an E-mail in the court, its evidentiary value is also a significant legal question. Article 9(2) of the UNCITRAL Model Law recognizes electronic messages as evidence but lays down certain factors to assess their evidentiary value :-

“Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.”

Promod Mahajan Case in India.

“Electronic record, data & Electronic form in I.T. Act”:-

(o)"Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

(r) "Electronic Form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(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;

Reading the aforesaid definitions of “electronic record”, “data” and “electronic form” in the I.T. Act, 2000 along with the definition of ‘document’ in the Indian Evidence Act, 1872, it becomes clear that computer images, text and sound stored, whether on a computer file, blog, web-site or e-mail, are all documents.

State vs. Mohd. Afzal Case : If someone challenges the accuracy of computer evidence on the ground of misuse of system or operating failure or interpolation, then the challenger has to establish the challenge. Mere theoretical and generic doubts cannot be cast on the evidence.

Best evidence rule deals with the nature or character of particular evidence which is considered for the purpose of arising at a rational conclusion. In State vs. Navjot Singh, (2005) 11 SCC 600 & P. Padmanabh vs. Syndicate Bank Ltd., Bangalore — AIR 2008 Kant. 42 it was held that the non compliance of 65B of Evidence Act is not always fatal if secondary evidence can be given in any circumstances.

One Computer forensics experts does the following;

- 1)Identifying sources of documentary or other digital evidence,**
- 2)Preserve the evidence,**
- 3)Analyze the evidence ,**
- 4)Present the findings.**

The Digital Evidence has to follow the following Rules:

- Admissibility,**
- Authenticity,**
- Completeness,**
- Reliability,**
- Believability**

Construction by pleadings, proof by evidence: proof only by relevant and admissible evidence. Genuineness, veracity or reliability of the evidence is seen by the court only after the stage of relevancy and admissibility. These are some of the first principles of evidence.

**: Anvar P.V. vs. P.K. Basheer and Others (2014)
10 SCC 473**

:Amendment of Evidence Act:

In section 3,— (a) in the definition of “Evidence”, for the words “all documents produced for the inspection of the Court”, the words “all documents including electronic records produced for the inspection of the Court” shall be substituted.

22A. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.”

Federal rules of evidence (2014): Rule 1003. Admissibility of Duplicates

A duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity or the circumstances make it unfair to admit the duplicate.

Some Similarity with section 22A. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question."

“59. Proof of facts by oral evidence.—All facts, except the contents of documents or electronic records, may be proved by oral evidence.

“65A. Special provisions as to evidence relating to electronic record: The contents of electronic records may be proved in accordance with the provisions of section 65B.”

65B. (1) Notwithstanding anything contained in this Act, 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 (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

**(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—
(a) by a combination of computers operating over that period; or**

**(b) by different computers operating in succession over that period; or
(c) by different combinations of computers operating in succession over that period; or**

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,—

(a) identifying the electronic record containing the statement and describing the manners in which it was produced.

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it. (5) For the purposes of this section,—

(a) information shall taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities, by a computer operated otherwise than in the course of those that information, of duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process.'

Certificate u/s 65B of Indian Evidence Act issued in relation to the CD titled “CCTV Footage”

I, the undersigned, state to the best of my knowledge and belief that:

1. The CD titled “CCTV Footage” being the copy of CCTV footage of the incidence dated _____ issued on _____ contains information stored in the computer system being used by our company to record the day to day incidence at our _____ at _____.

2. The said CD titled “CCTV Footage” has been produced by the said computer system during the period over which the computer system was used regularly to store and process information for the purposes of activities regularly carried on over that period by lawfully authorised persons.

3. That during said period, information of the kind contained in the electronic record was regularly fed into the said computer system in the ordinary course of the said activities.

4. I also affirm that throughout the material part of said period, the concerned computer was operating properly.

5. The information contained in the electronic record reproduces such information fed into the computer in the ordinary course of the said activities.

6. I am in a responsible official position in relation to the operation of the computer system.

Signed on this _____ July, 2014

(Mr. _____)

(Designation)

(Company Name)

Certificate u/s 65B of Indian Evidence Act issued in relation to the Printout of the downloaded copy of _____ dated _____ downloaded from email account of Mr. _____ having email account id. _____.

I, Mr. _____ son of _____ working residing at _____ state to the best of my knowledge and belief that:

1. That the related printout of the downloaded copy of _____ dated _____ downloaded from my email account having email account no. _____ was produced by my computer having model no. _____, _____ colour, made by _____, having battery model no. _____ during the period over which the said computer was used regularly to store or process information for the purpose of any activities regularly carried on over that period by me having lawful control over the use of my computer. The printout of the downloaded copy of _____ (which identifies the electronic record containing the statement) was taken from my own printer having model no. _____, _____ colour, made by _____ dully attached with my computer.

2. That the information produced by my computer system during the period over which the computer system was used regularly to store and process information for the purposes of different activities of day to day incidence regularly carried on over that period by me.

3. That during said period, information of the kind contained in the electronic record was regularly fed into the said computer system in the ordinary course of the said activities.

4. I also affirm that throughout the material part of said period, the concerned computer was operating properly.

5. That the information contained in the electronic record reproduces such information fed into the computer in the ordinary course of the said activities.

That the statements made above are true to my best knowledge and belief.

Signed on this _____ September, 2014

(Mr. _____)

Under Section 65B(4) of the Evidence Act, if it is desired to give a statement in any proceedings pertaining to an electronic record, it is permissible provided the following conditions are satisfied:

(a) There must be a certificate which identifies the electronic record containing the statement;

(b) The certificate must describe the manner in which the electronic record was produced;

(c) The certificate must furnish the particulars of the device involved in the production of that record;

(d) The certificate must deal with the applicable conditions mentioned under Section 65B(2) of the Evidence Act; and

(e) The certificate must be signed by a person occupying a responsible official position in relation to the operation of the relevant device.

88A. The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

90A. Where any electronic record, purporting or proved to be five years old, is produced from any custody which the court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorised by him in this behalf.

“Ziyauddin Burhanuddin Bukhari v. Brijmohan Ramdass Mehra & Ors, AIR 1975 SC 1788”:-

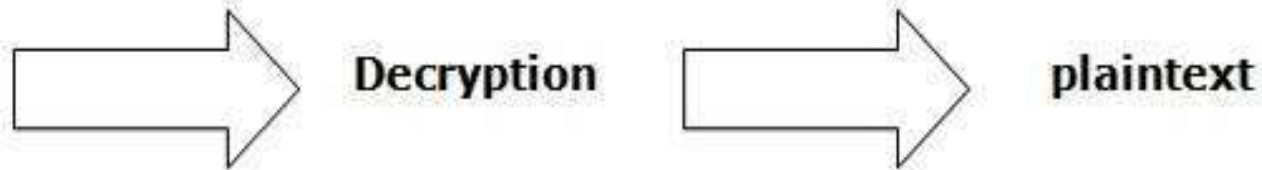
On a parity of reasoning, electronic records, whether in the form of text, images or sound stored, are also documents, irrespective of the storage media.

Hon'ble High Court at Delhi in Dharambir vs. CBI [148(2008) DLT 289] observed that Harddisk is a document combining the section 3 of the Indian Evidence Act and section 2(o) and (t) of IT Act

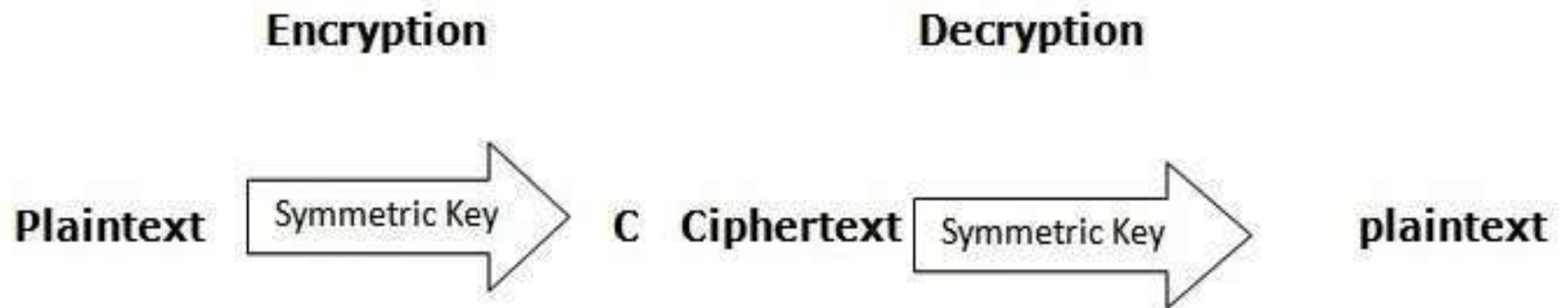
:Authentication:

The most important criticism on digital evidence is that digital evidence base can be easily altered.

However in US v. Bonallo (858 F. 2d 1427 - 1988 - Court of Appeals, 9th 2002) a US court ruled that "the fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness".



Basic Mechanism of Encryption



:Mechanism of Cryptography:

Dear, my ATM
password is attitude
and my account no.
123456

Plain text

Encryption

gghghghjgjtddtgnxgx
hghbhghgxghghgxhb
fxbxbfxbfxbfxbfxbfxb
ffxfxfxff&*sg&*

Ciphertext

Decryption

Dear, my ATM
password is attitude
and my account no.
123456

Plaintext

Laws of Digital Signature

3. Authentication of Electronic Records -

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation - For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

(a) To derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) That two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

3-A. Electronic Signature

- ¢ **(1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section(2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which -**
 - ¢ **(a) Is considered reliable; and**
 - ¢ **(b) May be specified in the Second Schedule**
- ¢ **(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if-**
 - ¢ **(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and of no other person;**
 - ¢ **(b) The signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;**
 - ¢ **(c) Any alteration to the electronic signature made after affixing such signature is detectable;**
 - ¢ **(d) Any alteration to the information made after its authentication by electronic signature is detectable; and**

- ¢ **(e) It fulfils such other conditions which may be prescribed.**
- ¢ **(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.**
- ¢ **(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the second schedule;**
- ¢ **Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.**
- ¢ **(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament**

5. Legal recognition of Electronic Signature. -

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.

Explanation - For the purposes of this section, "Signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "Signature" shall be construed accordingly.

79-A. Central Government to notify Examiner of Electronic Evidence.-

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation:- For the purpose of this section, "Electronic Form Evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines".

Section 45A of Evidence Act :Opinion of Examiner of Electronic Evidence- When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000(21 of 2000)., is a relevant fact. Explanation.—For the purposes of this section, an Examiner of Electronic Evidence shall be an expert.

Locard's Exchange Principle: The concept known as the "Locard's Exchange Principle" states that every time someone enters an environment, something is added to and removed from it. The principle is sometimes stated as "every contact leaves a trace", and applies to contact between individuals as well as between individuals and a physical environment. Law enforcement investigators are therefore taught to always assume that physical evidence is left behind at every scene.

Relevant Judgements

State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru((2005) 11 SCC 600):

“.....Irrespective of the compliance with the requirements of Section 65-B, which is a provision dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely, Sections 63 and 65. It may be that the certificate containing the details in sub-section (4) of Section 65-B is not filed in the instant case, but that does not mean that secondary evidence cannot be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely, Sections 63 and 65.”

Most importantly, such a certificate must accompany the electronic record like computer printout, Compact Disc (CD), Video Compact Disc (VCD), pen drive, etc., pertaining to which a statement is sought to be given in evidence, when the same is produced in evidence. All these safeguards are taken to ensure the source and authenticity, which are the two hallmarks pertaining to electronic record sought to be used as evidence. Electronic records being more susceptible to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice.

An electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under Section 65B are satisfied. Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible.

Any documentary evidence by way of an electronic record under the Evidence Act, in view of Sections 59 and 65A, can be proved only in accordance with the procedure prescribed under Section 65B. Section 65B deals with the admissibility of the electronic record. The purpose of these provisions is to sanctify secondary evidence in electronic form, generated by a computer.

.....Thus, notwithstanding anything contained in the Evidence Act, 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 a document only if the conditions mentioned under sub-Section (2) are satisfied, without further proof or production of the original. The very admissibility of such a document, i.e., electronic record which is called as computer output, depends on the satisfaction of the four conditions under Section 65B(2).

Anvar P.V. vs. P.K. Basheer and Others (2014) 10 SCC 473

The “doctrine of ‘prospective overruling’” on Electronic Evidence Laws

**IN THE SUPREME COURT OF INDIA
CRIMINAL APPELLATE JURISDICTION
CRIMINAL APPEAL No. 1418 of 2013
SONU @ AMAR Appellant(s)**

Versus

STATE OF HARYANARespondent(s)

With

**CRIMINAL APPEAL No.1416 of 2013
CRIMINAL APPEAL No. 1653 of 2014
CRIMINAL APPEAL No. 1652 of 2014**

“The interpretation of Section 65B (4) by this Court by a judgment dated 04.08.2005 in Navjot Sandhu held the field till it was overruled on 18.09.2014 in Anvar’s case. All the criminal courts in this country are bound to follow the law as interpreted by this Court. Because of the interpretation of Section 65B in Navjot Sandhu, there was no necessity of a certificate for proving electronic records. A large number of trials have been held during the period between 04.08.2005 and 18.09.2014. Electronic records without a certificate might have been adduced in evidence. There is no doubt that the judgment of this Court in Anvar’s case has to be retrospective in operation unless the judicial tool of ‘prospective overruling’ is applied. However, retrospective application of the judgment is not in the interests of administration of

justice as it would necessitate the reopening of a large number of criminal cases. Criminal cases decided on the basis of electronic records 29 adduced in evidence without certification have to be revisited as and when objections are taken by the accused at the appellate stage. Attempts will be made to reopen cases which have become final.”

“This Court did not apply the principle of prospective overruling in Anvar’s case. The dilemma is whether we should. This Court in K. Madhav Reddy v. State of Andhra Pradesh, (2014) 6 SCC 537 held that an earlier judgment would be prospective taking note of the ramifications of its retrospective operation. If the judgment in the case of Anvar is applied retrospectively, it would result in unscrambling past transactions and adversely affecting the administration of justice. As Anvar’s case was decided by a Three Judge Bench, propriety demands that we refrain from declaring that the judgment would be prospective in operation. We leave it open to be decided in an appropriate case by a Three Judge Bench. In any event, this question is not germane for adjudication of the present dispute in view of the adjudication of the other issues against the accused.”

THE BANKER'S BOOKS EVIDENCE ACT, 1891

'(3) "bankers' books" include ledgers, day-books, cash-books, account-books and all other books used in the ordinary bussiness of a bank whether kept in the written form or as printouts of data stored in a floppy disc, tape or any other form of electro-magnetic data storage device;'

2A. Conditions in the printout.—

1[2A. Conditions in the printout.—A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by the following, namely:—

▪

12A. Conditions in the printout.—A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by the following, namely:—(a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and

(b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of—

(A) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;

(B) the safeguards adopted to prevent and detect unauthorised change of data;

(C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;

(D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;
(E) the mode of verification in order to ensure that data has been accurately transferred to such removable media;
(F) the mode of identification of such data storage devices;
(G) the arrangements for the storage and custody of such storage devices;
(H) the safeguards to prevent and detect any tampering with the system; and(I) any other factor which will vouch for the integrity and accuracy of the system.
(c) a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data.]

Laws against Money Laundering on Online Banking:

The USA PATRIOT Act is an Act of Congress that was signed into law by President George W. Bush on October 26, 2001. The PATRIOT Act made a number of changes to U.S. law. Key acts changed were the

***Foreign Intelligence Surveillance Act of 1978*(FISA),
the *Electronic Communications Privacy Act of 1986*(ECPA),
the *Money Laundering Control Act of 1986* and
Bank Secrecy Act(BSA), as well as the
Immigration and Nationality Act.**

Prevention of Money-Laundering Act, 2002 (PMLA)

'Know Your Customer' (KYC) Guidelines - Anti Money Laundering Standards : RBI-2004-05/284,DBOD.NO.AML.BC.58/14.01.001/2004-05 November 29, 2004.

**Guidelines on 'Know Your Customer' norms
And Anti-Money Laundering Measures.**

(<http://www.iba.org.in/rbikycguidlines.asp>)

**Provisions of Section 66A STRUCK DOWN:
IN THE SUPREME COURT OF INDIA
CRIMINAL/CIVIL ORIGINAL JURISDICTION
WRIT PETITION (CRIMINAL) NO.167 OF 2012
SHREYA SINGHAL ... PETITIONER
VERSUS
UNION OF INDIA ... RESPONDENT**

The Supreme Court in a landmark judgement, struck down section 66A IT Act upholding freedom of expression and observes it "clearly affects" the fundamental right to freedom of speech and expression enshrined under Article 19 of the Constitution. The judgement says:

"119. In conclusion, we may summarise what has been held by us above: (a) Section 66A of the Information Technology Act, 2000 is struck down in its entirety being violative of Article 19(1)(a) and not saved under Article 19(2)."

Now what next?

The following provisions of law will always be there to protect one from the misuse of the social media.

1) Article 19(2) of Indian Constitution

2) Section 268, 292 – 294, 499 to 509 IPC etc.

3) Other provisions of IT and ITA Acts

a) Message violation of privacy: Section 66E ITA Act

b) Message or online activity against decency or morality, public order, defamatory against state: 66F ITA.

c) Transmitting obscene/sexuality explicit messages (women/child): 67, 67A, 67B ITA Act

d) Liability of intermediary like online social media; 79 ITA Act, 2008.

Section 66A of the Information Technology Act, 2000 is struck down in its entirety being violative of Article 19(1)(a) and not saved under Article 19(2).

Section 69A and the Information Technology (Procedure & Safeguards for Blocking for Access of Information by Public) Rules 2009 are constitutionally valid.

Section 79 is valid subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material.

The Information Technology “Intermediary Guidelines” Rules, 2011 are valid subject to Rule 3 sub-rule(4) being read down in the same manner as indicated in the judgment.

SUPREME COURT OF CANADA

R. v. SPENCER, 2014 SCC 43, [2014] S.C.R. 212

“.....Constitutional law — Charter of Rights — Search and seizure — Privacy — Police having information that IP address used to access or download child pornography — Police asking Internet service provider to voluntarily provide name and address of subscriber assigned to IP address — Police using information to obtain search warrant for accused’s residence — Whether police conducted unconstitutional search by obtaining subscriber information matching IP address — Whether evidence obtained as a result should be excluded.....

Judgement on Cyber Defamation:

Vyakti Vikas Kendra, India Public ... vs Jitender Bagga & Anr on 9 May, 2012, Delhi High Court, Manmohan Singh, CS(OS) No.1340/2012

..... The four plaintiffs, namely, Vyakti Vikas Kendra, India Public Charitable Trust, Mr Gautam Vig, Mrs. Bhanumati Narsimhan and Mrs. Sharmila Murarka, have filed present suit against the defendants for damages to tune of Rs.5,09,00,000/-, permanent and mandatory injunction, mainly on the ground that they are aggrieved, hurt and immensely concerned on account of certain highly defamatory materials posted on an internet website by the name <http://www.blogger.com/> by one Mr Jitender Bagga, the defendant No.1 herein. The said website is owned by Google, the defendant No.2. It is a Blog Publishing Service which allows people to create and publish a "Blog".

Delhi High Court
Raj Kumar vs State on 19 April, 2016

IN THE HIGH COURT OF DELHI AT NEW DELHI

Judgment Reserved on: April 07, 2016

Judgment Delivered on: April 19, 2016

CRL.A. 232/2016

RAJ KUMAR

..... Appellant

versus

STATE

..... Respondent

CORAM:

HON'BLE MR. JUSTICE PRADEEP NANDRAJOG

HON'BLE MS. JUSTICE MUKTA GUPTA

MUKTA GUPTA, J.

.....The photograph alleged to be bone of contention was not admissible in evidence for want of certificate under Section 65-B of the India Evidence Act.....

.....He produced his mobile phone with a photograph to the Police which was seized vide seizure memo Ex.PW-3/A. He identified the mobile phone and the photograph therein before the Court.....

..... Since the mobile phone of Hemraj itself has been produced in the Court and exhibited, there was no need of a certificate under Section 65B Indian Evidence Act.....

Citation : *Raj Kumar v. State, CRL.A. 232/16*, 19.4.16 DHC

Anoushka Shankar's Case Studies:

¢ **Allegation:** Email hacked into by an offender who took control of some very private photographs stored in the inbox of the email and blackmailed and threatened via email by some unknown person that he would make some of her photographs public found in her email inbox, if his demand of \$ 100,000 was not paid by her.

¢ **Step:** Inspector Pawan Kumar under the supervision of ACP Sanjeev Yadav elite Special Cell of Delhi Police took up investigation.

¢ **Investigation:** 1) The special cell cops traced the internet protocol address (IP address) from which the Emails were sent.

- ¢ **2) The extortive emails sent by the offender were found to be sent mostly from Gmail Account.**
- ¢ **3) Though the Gmail blocks the IP address of the sender and it is not visible to the recipient of the email. However, one email was found to be from other email service provider and it was found that it had been sent from India; rest of the emails were found to be from Dubai, elsewhere in the UAE, and the USA.**
- ¢ **4) The police tracked down one of the IP address to a residential address located at MUMBAI and nabbed the accused person, whose name came to be known as Junaid Jameel Ahmed Khan who confessed to his crime.**
- ¢ **5) The cops seized the hard disk of the computer from which the alleged emails were sent, prepared the mirror image of the same and the hard disk was sent to the Forensic Science Laboratory, Hyderabad for further analysis.**

- ¢ **6) The cops also seized the passport of the offender through which it was found that the offender was at Dubai on the same date when the extortive emails from Dubai were received by Anoushka, which clearly corroborates the offence committed by the offender.**
- ¢ **7) The Special Cell cops registered the case under Section 386 Indian Penal Code which deals with offence of extortion. The accused hacked into the email of the Anoushka, Section 66 IT Act has been added as the same is attracted to the offence.**

- ¢ **8) The material evidence seized by the cops proves the involvement of the offender as the IP address has been traced to his residence.**
- ¢ **9) The examination and analysis of the seized hard disk of the computer of offender at the forensic laboratory would prove that the emails have been hacked into and photographed copied by the offender from the inbox of the email. If it is further revealed by the analysis of the hard disk that the photographs found in the possession of the offender, have been transmitted by him electronically, say some of his friends, the same would amount to publication in electronic form which would be squarely covered and punishable under section 67 of IT Act.**
- ¢ **The activities on the internet leaves a footprint through which the accused can be traced and brought to justice.**

Bivas Chatterjee
Edit Profile

- FAVORITES
- News Feed
 - Messages 20+
 - Events
 - Photos
 - Cyber Crime Aware... 1
 - Saved 1

- GROUPS
- Cyber Crime Inve... 20+
 - Calcutta High Cou... 20+
 - cyber crime detect... 20+
 - Sri Ma Sarada Devi 20+
 - Faculty of law, uni... 20+
 - Cyber Law & Infor... 20+
 - Advocate (অধিবক্তা) 20+
 - EC Council Kolkata 7
 - CHILEKOTHA 20+
 - ALIPORE JUDGES... 17
 - New Groups 20+
 - Create Group


FRIENDS

- Computer Hacking ...

Update Status Add Photos/Video Create Photo Album

 What's on your mind?

Public Post

 **Pritam Nag** ▸ **Sri Ma Sarada Devi**
46 mins · 🌐

যেই রাম সেই কৃষ্ণ মিলেমিসে রামকৃষ্ণ,, আজ ঠাকুরের শুভ জন্মতিথি তে ঠাকুরের শ্রী চরনে শতকোটি প্রণাম



 Sanjit Bera and 11 others

- TRENDING
-  **InSight:** NASA Reschedules Space Mission to Mars for May 2018
 -  **Vijay Mallya:** Attorney General Says Indian Businessman Left Country on March 2
 -  **Open Compute Project:** Google Joins Initiative to Share Data Center Technology
- See More

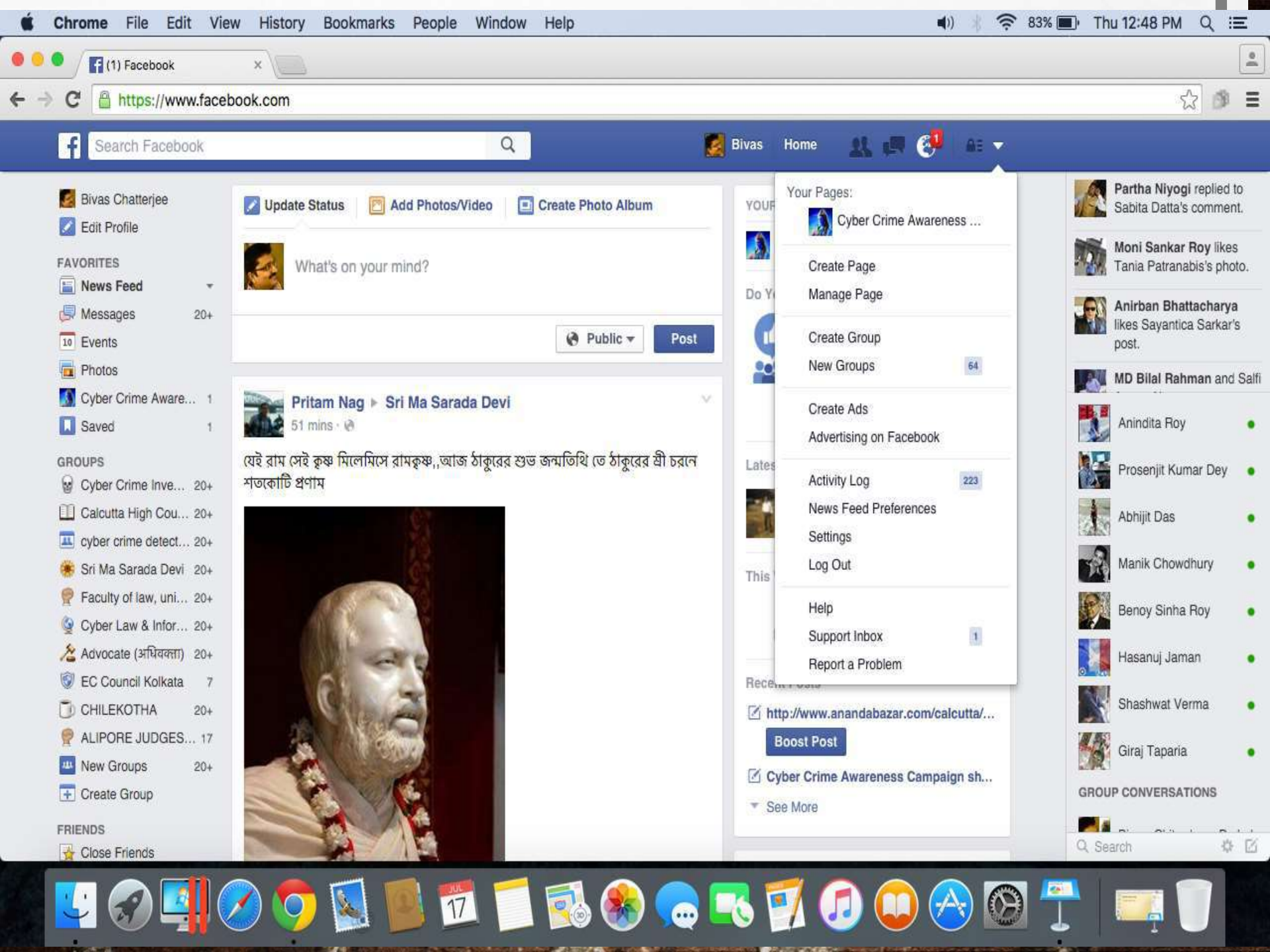
FRIEND REQUESTS See All

-  **Harabilash Roy**
4 mutual friends

-  **Sad Sadb**
Subodh Ch Saha is a mutual friend.

-  **Sankar Saha**
2 mutual friends

-  **Suman Saha**



General

Security

Privacy

Timeline and Tagging

Blocking

Language

Notifications

Mobile

Public Posts

Apps

Ads

Payments

Support Inbox

Videos

General Account Settings

Name	Bivas Chatterjee	Edit
Username	http://www.facebook.com/bivas.chatterjee.5	Edit
Email	Primary: bivas.chatterjee@gmail.com	Edit
Password	Updated about 7 months ago.	Edit
Networks	No networks.	Edit
Temperature	Fahrenheit	Edit

[Download a copy of your Facebook data.](#)

Partha Niyogi replied to Sabita Datta's comment.

Moni Sankar Roy likes Tania Patranabis's photo.

Anirban Bhattacharya likes Sayantica Sarkar's post.

MD Bilal Rahman and Salfi

Adv Soumyadeep B...

Anindita Roy

Pratick Mukherjee

Prosenjit Kumar Dey

Avinash Almal

Manik Chowdhury

Hasanuj Jaman

Giraj Taparai

GROUP CONVERSATIONS

Search

Download Your Information

Get a copy of what you've shared on Facebook.

Start My Archive

What's included?

- Posts, photos and videos you've shared
- Your messages and chat conversations
- Info from the About section of your profile
- And more



- Partha Niyogi replied to Sabita Datta's comment.
- Moni Sankar Roy likes Tania Patranabis's photo.
- Anirban Bhattacharya likes Sayantica Sarkar's post.
- MD Bilal Rahman and Salfi
- Adv Soumyadeep B...
- Anindita Roy
- Pratick Mukherjee
- Prosenjit Kumar Dey
- Avinash Almal
- Manik Chowdhury
- Hasanuj Jaman
- Giraj Taparia

GROUP CONVERSATIONS

Search

Download Your Information

Get a copy of what you've shared

Start My

What's included?

- Posts, photos and videos you've shared
- Your messages and chat conversations
- Info from the About section of your profile
- And more

Request My Download

It may take a little while for us to gather your photos, wall posts, messages, and other information. We will then ask you to verify your identity in order to help protect the security of your account.

Start My Archive

Cancel

Download Your Information

Get a copy of what you've shared

We're generating your personal archive. We'll email you when it's ready.

What's included?

- Posts, photos and videos you've shared
- Your messages and chat conversations
- Info from the About section of your profile
- And more

Download Requested

We are gathering your information and will send an e-mail to bivas.chatterjee@gmail.com when it is ready for download.

Okay

- Partha Niyogi replied to Sabita Datta's comment
- Monti Sankar Roy likes Tania Patranabis's photo
- Anirban Bhattacharya likes Sayantica Sarkar's post.
- MD Bilal Rahman and
- Adv Soumyadeep B...
- Rahul Rathee
- Anindita Roy
- Pratick Mukherjee
- Prosenjit Kumar Dey
- Tumpa
- Manik Chowdhury
- Pramod Thakur

GROUP CONVERSATIONS

Search



Bivas



67



Gmail

More

11 of 23,580

COMPOSE

Your Facebook download is ready

Inbox x



Inbox (1,806)

Starred

Important

Sent Mail

Drafts (207)

Circles

Personal

Travel

More

Bivas

Ayan Boral

Kaka ki korcho



Facebook <notification+zj4oyzy0ccc6@facebookmail.com> [Unsubscribe](#)
to me

1:00 PM (11 hours ago)



You recently requested a copy of your Facebook data. It's now ready for you to download.

Because this download may contain private information, you should keep it secure and take precautions when storing or sending it, or uploading it to another service.

Click the link below to go directly to your download. If the link redirects you to your account settings page, simply click "Download a copy of your Facebook data" to get redirected to the file we've prepared.

Please note: For security reasons, you can only download the copy we've prepared for you within a few days of this email being sent. You'll need to start the process again if you're unable to access your download.

<https://www.facebook.com/dyi?x=AdnjcLoFDkUDXbdU>

This message was sent to **bivas.chatterjee@gmail.com**. If you don't want to receive these emails from Facebook in the future, please **unsubscribe**. Facebook, Inc., Attention: Community Support, Menlo Park, CA 94025

Download Your Information

Get a copy of what you've shared on Facebook.

This is a copy of personal information you've shared on Facebook. To protect your info, we'll ask you to re-enter your password to confirm that this is your account.

Download Archive

Caution: Protect your archive

Your Facebook archive includes sensitive info like your private Wall posts, photos and profile information. Please keep this in mind before storing or sending your archive.



- Krishna Nand Pandey** likes Abhijit Dutta's post.
- Avijit Roy** likes SFI Kolkata District Committee's photo.
- Rana Das** likes Kolkata 24x7 Live's link.
- Debnath Sadhukhan** likes Amit Kumar Mitra's photo.
- Sanjukta Dey**
- Swagata Guha Niogi** 3h
- Imtiaz Rahaman** 6h
- Debaditya Roy** 53m
- Adv Soumyadeep B...** 1h
- Nazmul Hassan Has...** 5h
- Rumki Nath**
- Gayatri Sarkar** 1h

GROUP CONVERSATIONS

THANKS FOR PAYING ATTENTION

BIVAS CHATTERJEE

SPECIAL PUBLIC PROSECUTOR

9830158159

Mail: bivas.Chatterjee@gmail.com

Twitter: [@cybercrimemanea](https://twitter.com/cybercrimemanea)

My Youtube Channel : <http://www.youtube.com/c/BivasChatterjee>