

E-MAIL CHEATING

MR. VIJAY NINWANE WORKS AT ABUDHABI

MADE FRIENDSHIP WITH “X” (A BEAUTIFUL GIRL)-CHATING,NUDE
PHOTOS,EROTIC STORIES.

“X” INTRODUCED HER FRIENDS Y1,Y2,Y3,Y4,-----

VIJAY COULDN'T MEET X AS PROMISED

X COMMITTED SUICIDE.

VIJAY RECEIVED MAIL FROM

WWW.KOLKATTA_POLICE.COM

WWW.CBI_HQ.COM

VIJAY CONTACTED Y1 FOR HELP

Y1 APPOINTED Mr. Pranab mitra of mitra & mitra associates leading
lawyers

TOTAL Rs.70 LAKHS (RS.1.19 CRORE AS PER I.O)

WHAT ANALYSIS REVEALED----

ALL WAS DONE BY A SINGLE MAN
NAMED MR.PRANAB MITRA,
GENERAL MANAGER, -----

CRIMINAL LAW (BASICS) ITS INTERFACE WITH CYBER CRIMES

BY

DR. KVK SANTHY

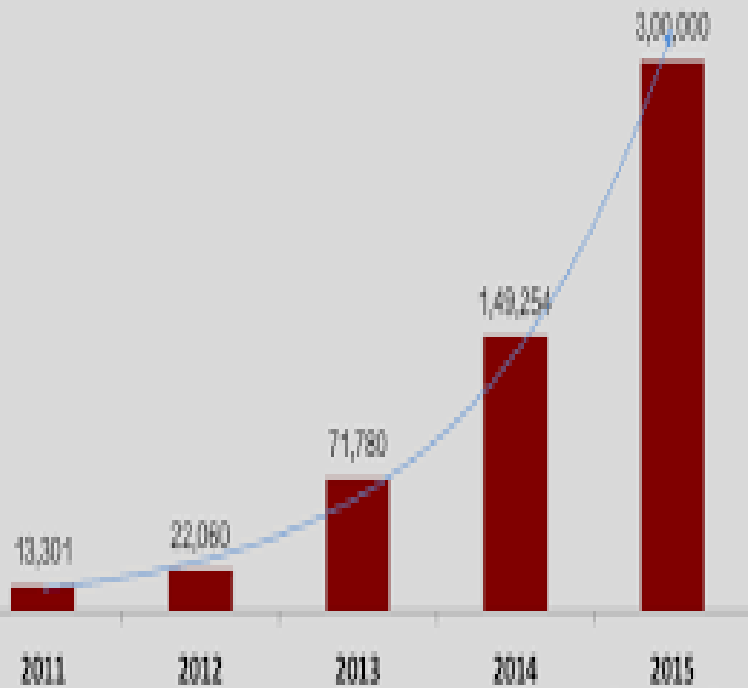
ASST. PROFESSOR

CRIMINAL LAW

NALSAR UNIVERSITY OF LAW

STATISTICS

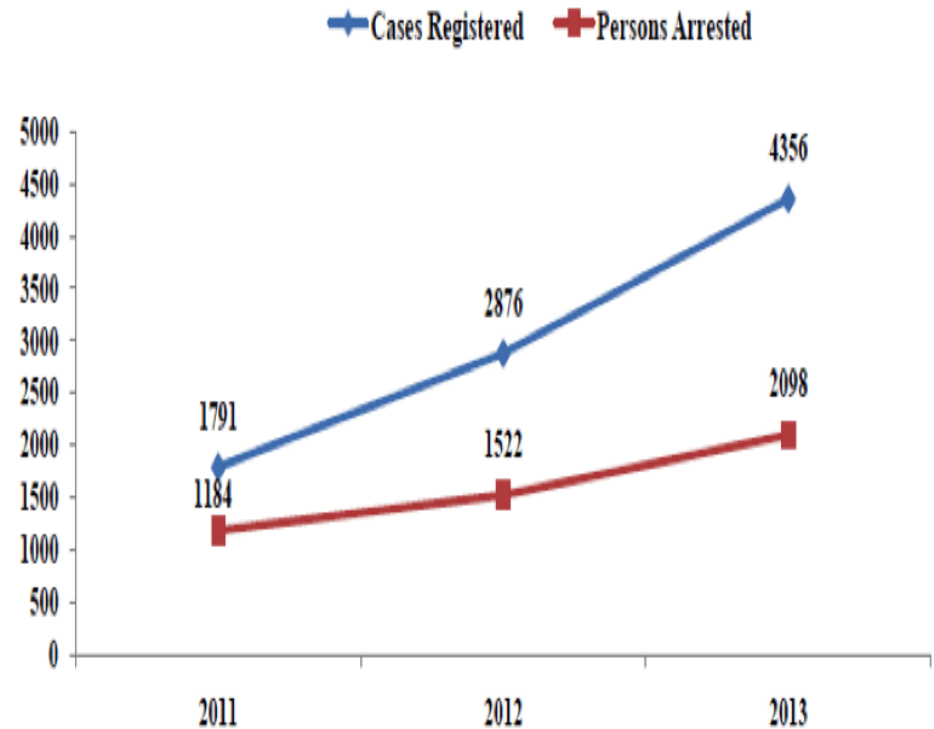
NUMBER OF CYBER CRIME CASES IN INDIA



SOURCE: ASSOCHAM-Mahindra SSG Report, Jan 2015

dazinfo

All India Cyber Crimes - Cases Registered Under IT Act (2011-13)

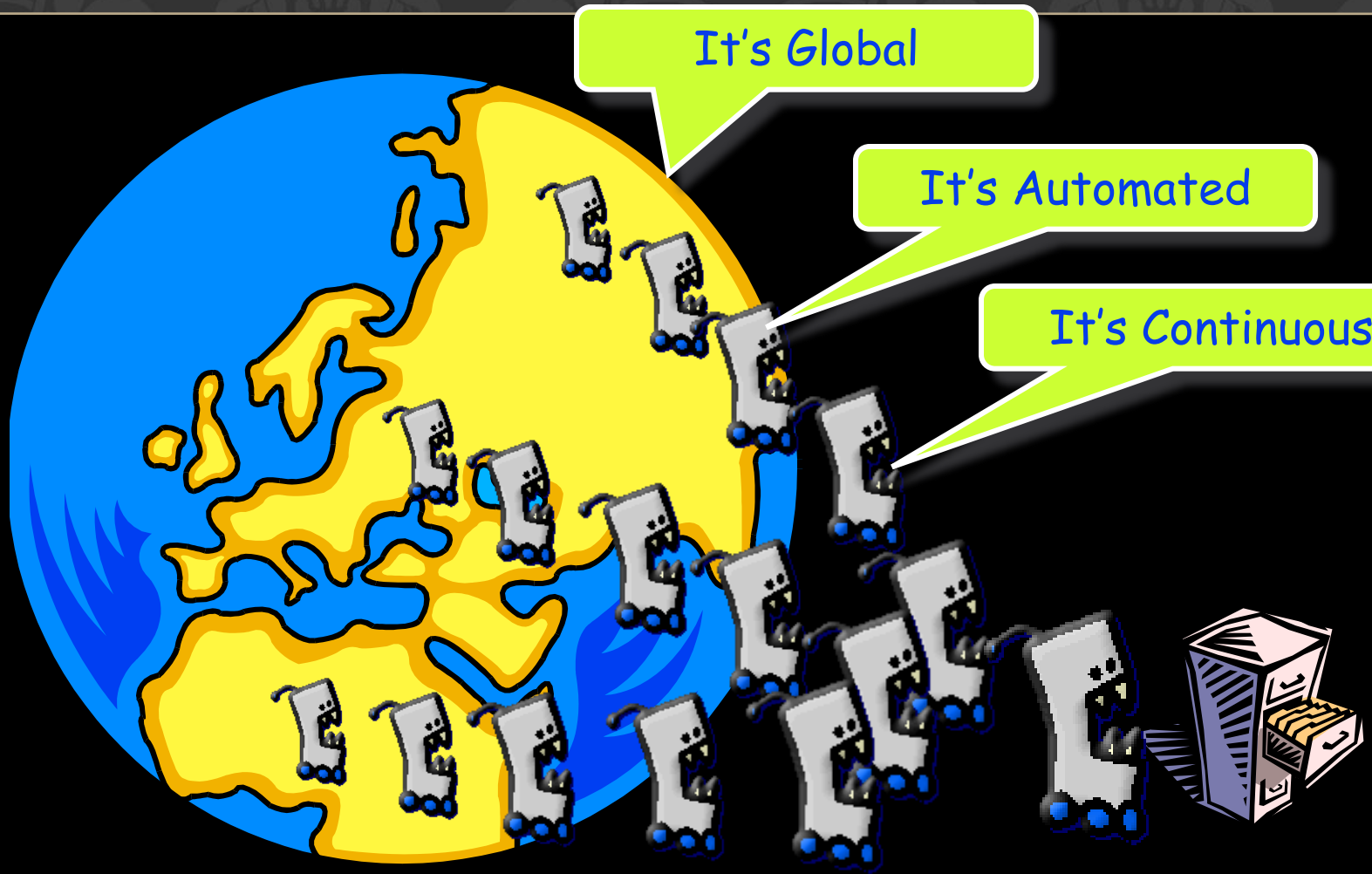


PECULIARITY OF CYBER CRIME

- Anonymity
- Almost no physical evidence/ clues
- High impact & intensity
- Many times far away from the scene of crime
- Jurisdictional Bars and sovereignty issues



WHY IS IT DIFFERENT?



DEFINING CYBER CRIME

(i) "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;

- All electronic devices.



“An unlawful act wherein the computer is used either as a tool or as a target or as both”

CYBER CRIMES

1.
Computer
Assisted

2.
Computer
Oriented



COMPUTER ASSISTED CYBER CRIMES

Selling non existent,
defective, substandard or
counterfeit goods,

Theft of credit card,

Bank fraud,

Fake stock shares,

Intellectual property
offences including
unauthorized sharing of
the copy righted content
of movies,music,
digitised books

COMPUTER ORIENTED CYBER CRIMES

Malicious
Software:
viruses, trojans
(which corrupt
server)

Cyber
terrorism

Child
pornography

Violent and
extreme
pornography

Internet
inspired
homicides and
suicides





CRIMES & JURISDICTION

- Determination of where the offence occurred is necessary to know which law to apply, secondly, obtaining evidence to try accused before a court.
- There are Complex legal problems of jurisdiction & extradition
- If an online financial newsletter of Bahamas contain fraudulent speculation about prospects of a company, whose share are traded on Australian Stock Exchange, where offence is committed?



ISSUES FOR ENFORCEMENT OFFICIALS

In early May of 2000, a computer virus known as the "love bug" emerged and spread rapidly around the globe. According to one report, the virus, which was designed to disseminate itself and to destroy various kinds of files on a victim's computer, "infected at least 270,000 computers in the first hours" after it was released, the "love bug" forced the shutdown of computers at large corporations such as Ford Motor Company and Dow Chemical Company, as well as the computer system at the House of Lord.

- It took days to arrest – no law
- Credit card law – finally held not applicable to hacking

ISSUES FOR ENFORCEMENT

- The **lack of cybercrime-specific penal laws** and/or the inadequacy of penal laws that were crafted to deal with criminal conduct occurring in the real, physical world, not in or by means of the virtual world of cyberspace;
- The **lack of international agreements** on cybercrimes which exacerbates the problems posed by the lack/inadequacy of local penal law and the often conflicting requirements local procedural laws;
- The difficulty of ascertaining **which nation(s) has/have jurisdiction** to prosecute a cybercriminal and, once this determination has been made, of asserting jurisdiction over that person;
- The difficulty of determining how many offenses have been committed, against whom and the damage resulting from those offenses.

CYBER CONSPIRACY

In August 2007, Mumbai teenager Adnan Patrawala was kidnapped from the suburbs and later found murdered in Nay Mumbai allegedly by friends he made on Orkut.

The 16-year-old boy was lured with a fake female on-line profile "Angel" to a late night meeting in a shopping mall.³³ He was then kidnapped and strangled to death, before his parents could pay the ransom.



NEW ADDITIONS IN 2008

S/66A-Punishment for sending offensive messages.

S/66B -Punishment for dishonestly receiving stolen computer resource.

S/66C-Punishment for identity theft.

S/66D-Punishment for cheating by personation by using computer resource.

S/66E-Punishment for violation of privacy.

S/66F-Punishment for cyber terrorism.

S/67A-Punishment for publishing or transmitting of material containing sexually explicit act.

S/67B -Punishment for child pornography.

HACKING



HACKING

- Section 65 deals with 'Tampering with computer source documents'.
- Section 66 deals with 'Hacking with Computer Systems'.

**Yesterday I
Changed My Wifi
Name To "Hack If
You Can" When I
checked It Today It
Was "Challenge
Accepted".**

11
11
01
11
11
01
10
01
00
01
00

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 programme, 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 two lakh rupees, or with both.

66. HACKING WITH COMPUTER SYSTEM.-

(1) Whoever with the **intent** to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or **diminishes its value or utility or affects** it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, **or with fine** which may extend up **to two lakh rupees**, or with both.

**SEC 66:. THE OFFENCE AS PER THIS
SECTION INVOLVES THE FOLLOWING
ELEMENTS:**

- **There should be intent on the part of the accused** to cause wrongful loss or damage to the public or any person.
- There should be knowledge of an attributable to the **accused that he is likely to cause wrongful loss or damage to the public or any person**
- The accused must **destroy or delete or alter any information** residing in a computer resource
- The **accused must diminish the value or utility** of any information residing in a computer resource
- The accused must affect any information residing in a computer resource injuriously by any means.

- Any person who breaches a protected system leaves himself open to criminal liability under section 70 IT Act. Any one who access or attempts to access a protected system commits an offence and can be punished with imprisonment for a term of ten years and can also be fined.).
- Hacking includes the following activities as per law.
- Unauthorized access to information systems
- **Disruption, interference**
- Introduction of malicious software
- Downloading, extraction copying
- Destroying altering info
- Stealing, concealing, altering computer source code. 1 crore, 3 yrs, 1 lakh

**VARPAUL SINGH VS. STATE OF
PUNJAB
(19.04.2010 - PHHC)**

- The petitioner was working in the capacity of General Manager of M/s Makkar Motor Private Limited. In furtherance of the common intention of the accused, fictitious bills and entries were created. Important data was deleted from the computers. Related documents were taken away by way of committing the offence of theft. Spare parts had been sold/ embezzled. Substantial amount has been pocketed by the accused mentioned in the FIR.
- Allegation is also to the effect that he misused the confidence reposed in him by way of giving him access to the main frame

**43 PENALTY AND COMPENSATION FOR DAMAGE TO
COMPUTER, COMPUTER SYSTEM, ETC (AMENDED
VIDE ITAA-2008)**

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network -

- (a) accesses or secures access to such computer, computer system or computer network or computer resource (ITAA2008)
- (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 programmes residing in such computer, computer system or computer network;
- (e) disrupts or causes disruption of any computer, computer system or computer network;

CONTD,

- (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 thereunder,
- (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 (Inserted vide ITAA-2008)**
- (i) 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, (Inserted vide ITAA 2008)

WHO IS HACKER?

- a hacker is ‘a person or thing that cuts roughly’ or ‘a person who uses computers for a hobby especially in gaining unauthorised access to data (Oxford English Dictionary): Six hackers are
- (a) A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to many users, who prefer to learn only the minimum necessary;
- (b) A person who enjoys the intellectual challenge of overcoming or circumventing limitations;
- (c) A person good at programming quickly;
- (d) An expert in a particular language;
- (e) A person who programs enthusiastically;
- (f) A malicious meddler who tries to discover sensitive information by poking around.

DATA DIDLING.....????? CRIME

INVOLVES ALTERING THE RAW DATA
JUST BEFORE A COMPUTER
PROCESSES IT AND THEN CHANGING
IT BACK AFTER PROCESSING IS
COMPLETED

SECONDARY STATE BOARD

PRIVATE STUDENTS TOPPED OVER
GOVT STUDENTS

6 DIGIT ROLL NUMBER

GOVT STUDENTS STARTS WITH 3

PRIVATE STUDENTS STARTS WITH 4
SOFTWARE MANIPULATION

FOR ROLL_NO 3 > 68 <= 100 DEDUCT 9

FOR ROLL_NO 4 > 68 < 88 ADD 9

MOBILE TELEPHONE COMPANY



CASE OF ICICI BANK

SUPPORT@ICICI.COM

Asked to validate or conform their account details for verification details

User id's, login password & transaction password

<http://infinity.icicibank.co.in/verify.jsp>

ON CLICKING

TWO WINDOWS

PRESS “VERIFY TAB”, THE WEB PAGE TAKES YOU TO <http://icici.com>
WHICH REDIRECTS TO www.icicibank.com

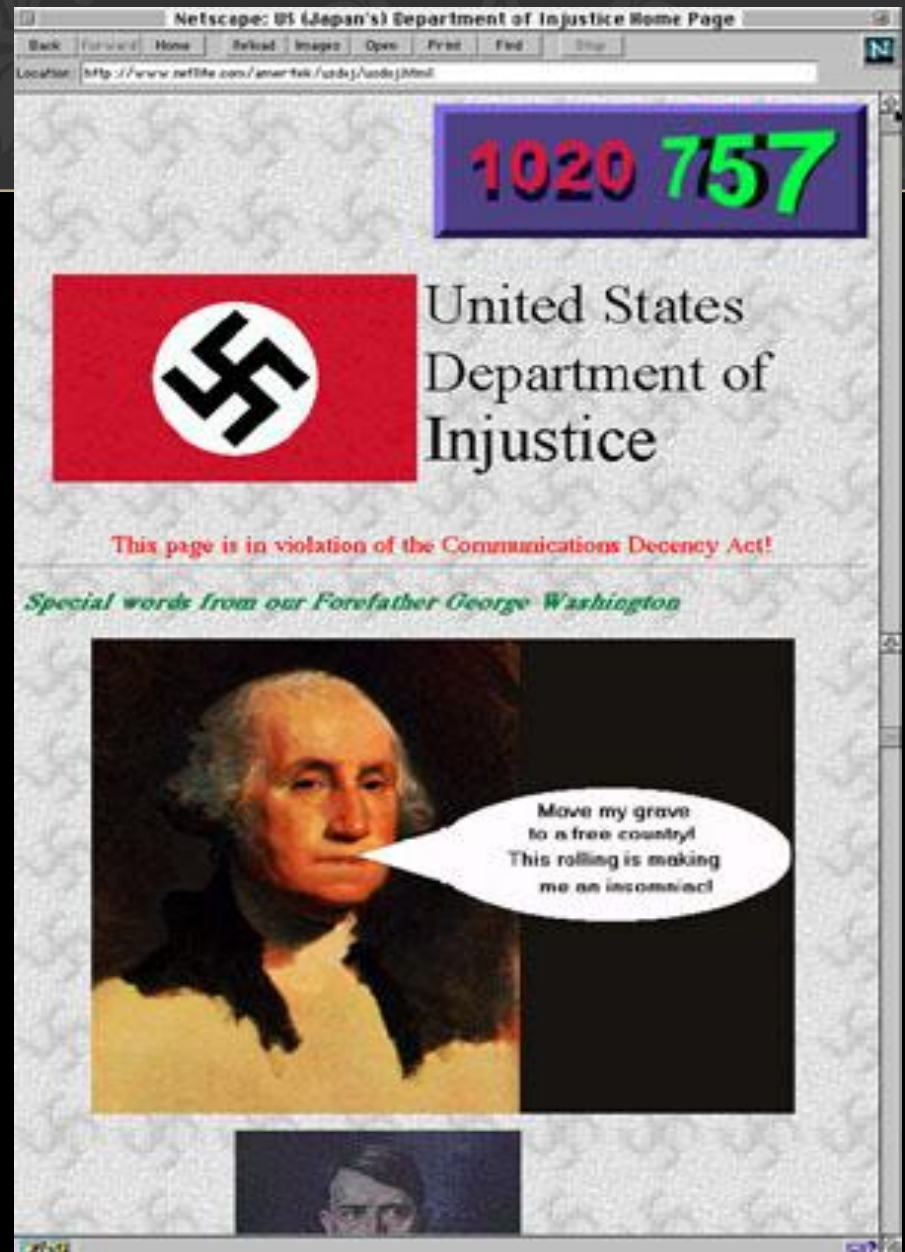
URL <http://all-about-notebooks.com/icici/verify.php>

ICICI NEITHER OWNS NOR IN ANY CONNECTED WITH THE SAID URL
IP ADDRESS 61.141.32.181

WEB DEFACEMENT

You've been
hacked...

Dept of Justice US



WEB DEFACEMENT

You've been
hacked...

CIA



DENIAL OF SERVICE

A METHOD OF ATTACK THAT DENIES SYSTEM ACCESS TO LEGITIMATE USERS

IT CAN PREVENT ONE SYSTEM FROM BEING ABLE TO EXCHANGE DATA WITH OTHER SYSTEMS OR PREVENT THE SYSTEM FROM USING THE INTERNET.



CYBER MURDER

- Hacked Liverpool hospital in 1994 and changed the medical prescriptions.
- A nine-year-old patient who was given a highly toxic mixture was saved by a nurse who decided to re-check his prescription.
- Wanted to see confusion and mayhem arising out of tampering with hospital computers.
- An underworld don who was injured by a gun shot was killed by a drug overdose which was caused by alteration of the original prescription by a hacker. (New York)
- A hacker altered 60 mg to 260 mg insulin prescription, led to death



CRIMES AND CYBER CRIMES ANALOGY

- IPC, Section 441: Criminal Trespass
- Unauthorized entry
- Unlawful stay
- Intention to commit crime
- S 43 + S 66 IT Act: Hacking
- Unauthorized access to information systems
- Disruption, interference
- Introduction of malicious software
- Downloading, extraction copying
- Destroying altering info
- Stealing, concealing, altering computer source code. 1 crore, 3 yrs, 1 lakh

SEXUAL OFFENCES – CYBER SPACE

Sec 66A: Cyber Stalking

Sec. 67A. Publishing of information which is obscene in electronic form.

Sec. 67B : Child Pornography



1. CYBER STALKING

- Cyber stalking is the use of the internet, e-mail or other electronic communication devices to stalk another person.
- Repeated threatening, harassing phone calls, sending harassing messages or objects or even destroying victim's property.
- Track their targets through the net in chatrooms, message boards, newsgroups or even mailing lists in which their victims actively take part. befriending their target's friend's to get more information about victims.



**66 A PUNISHMENT FOR SENDING OFFENSIVE MESSAGES THROUGH
COMMUNICATION SERVICE, ETC.**

(Introduced vide ITAA 2008)

Any person who sends, by means of a computer resource or a communication device,-

- a) any **information** that is grossly offensive or has menacing character; or
- b) any **information** which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes **by making** use of such computer resource or a communication device,
- c) any **electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008)**

shall be punishable with imprisonment for a term which may extend to two **three** years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

RITU KOHLI

Ritu Kohli, registered first cyber stalking case.

A friend of her husband gave her phone number and name on a chat site for immoral purposes.

Being a computer expert, Kohli was able to trace the culprit.

Trial began for "outraging the modesty of a woman", under Section 509 of IPC.



TWEET AT YOUR OWN RISK IN INDIA

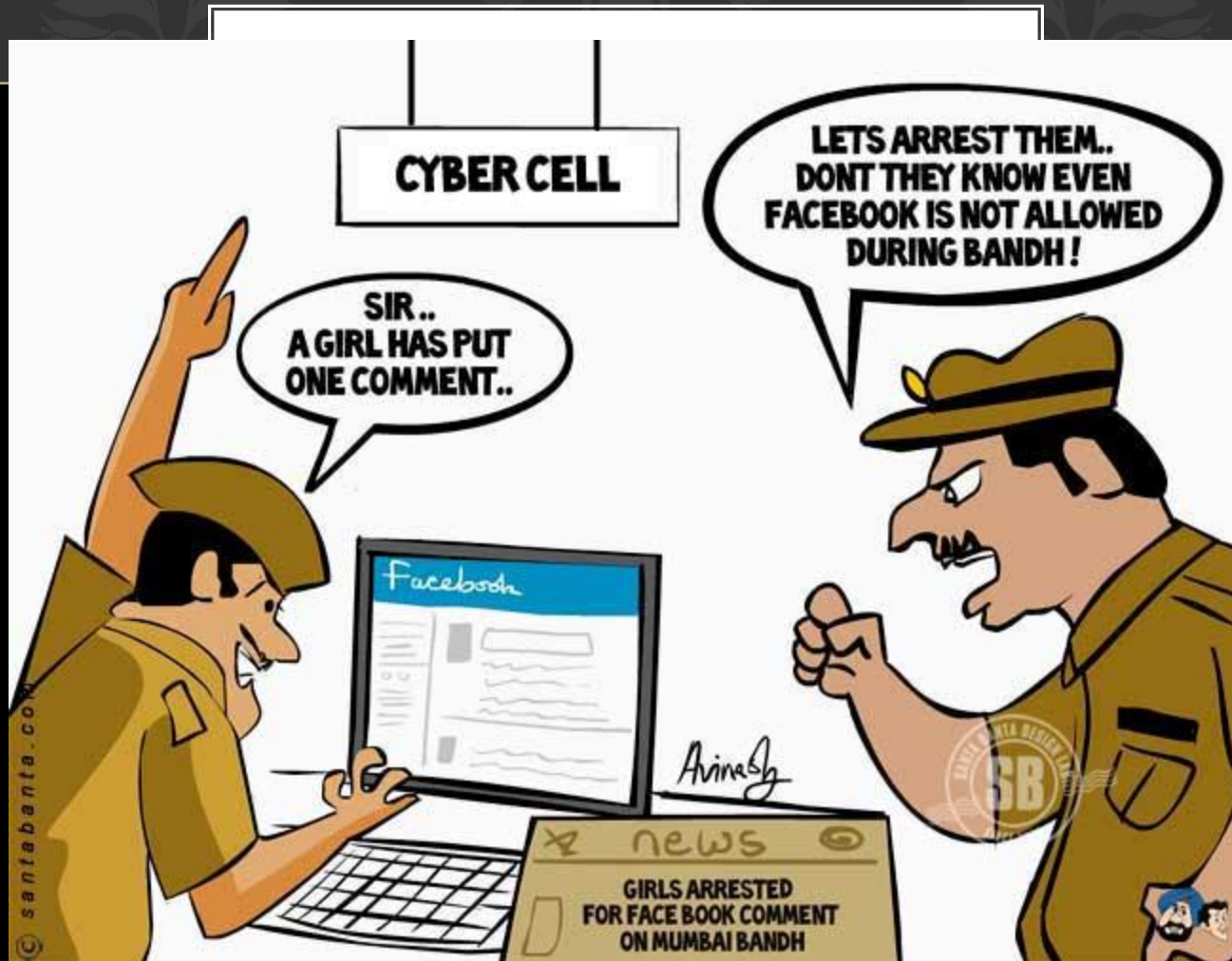
GIRLS ARRESTED



KIN THREATENED

PALGHAR





SHREYA SINGHAL



**SHREYA SINGHAL V. UNION OF
INDIA, (2013) 12 SCC 73**

- The first PIL on the issue was filed in 2012 by a law student Shreya Singhal, who sought amendment in Section 66A of the Act. This was filed after two girls - Shaheen Dhada and Rinu Srinivasan - were arrested in Palghar in Thane district as one of them posted a comment against the shutdown in Mumbai following Shiv Sena leader Bal Thackeray's death and the other 'liked' it.
- Sec 66 A was struck down as its violating Art19(1) of Constitution. (Rohinton Nariman)

MISUSE OF THE LAW

1. Jadavpur University professor **Ambikesh Mahapatra** was arrested for forwarding caricatures on Trinamool Congress chief Mamata Banerjee on Facebook in 2012.
2. Activist **Aseem Trivedi** was also arrested in 2012 for drawing cartoons of Parliament and the Constitution to depict their ineffectiveness. He was arrested on charges of sedition leading to huge protests.
3. In another instance in 2012, **Air India employee Mayank Sharma and KV Rao** from Mumbai were arrested for allegedly posting offensive comments against politicians on their Facebook group.
4. Businessman **Ravi Srinivasan** was also charged in 2012 by Puducherry Police for allegedly tweeting against Karti Chidambaram, son of then union minister P Chidambaram. he had allegedly called Karti 'corrupt' in his tweet.

5. In 2012, **three youngsters from Kishtwar** district - Kishori Sharma, Bansi Lal and Moti Lal Sharma - were arrested and sent to jail for 40 days after they were tagged in an allegedly blasphemous video posted on Facebook. One of them had commented on the post. They were charged with desecrating religious symbols and inciting communal hatred by using information technology.

6. A **tourism officer in Varanasi** was arrested for uploading "objectionable" pictures of Samajwadi Party chief **Mulayam Singh Yadav**, Uttar Pradesh Chief Minister Akhilesh Yadav and senior SP leader Azam Khan on Facebook.

7. In August 2013, poet and writer **Kanwal Bharti** was arrested by police for posting a message on Facebook that criticised the Uttar Pradesh government for suspending IAS officer Durga Shakti Nagpal, who had cracked down on the sand mafia. Bharti's post questioned why Nagpal had been suspended for ordering the demolition of a wall intended to be part of a mosque while no officer in Rampur was dismissed when an old madrasa was pulled down. He said the reason was because the town was controlled by Samajwadi Party leader Azam Khan.

8. In 2014, a young shipping professional **Devu Chodankar** was booked for a Facebook post on **Prime Minister-elect Narendra Modi** in which he said that would start a holocaust in India. Chodankar had written on a Facebook forum on Goa+, a popular forum with over 47,000 members, if elected to power, Modi would unleash a 'holocaust'. He deleted his post subsequently. Chodankar later apologised for his choice of words but stood by the sum of his argument, calling it his crusade against the "tyranny of fascists".

. Police arrested CPI-M worker **Rajeesh Kumar** for posting "abusive" comments and photos on Facebook about Prime Minister Narendra Modi. Police said in one of the posts, Modi was depicted in a picture shown with an imprint of a shoe on his face. They claimed the posts had abusive comments against Modi and a comment in one post could have sparked communal tensions.

10. Recently, a class 11 student was arrested for making a Facebook post about UP minister Azam Khan. Khan had claimed that law is enforced with strictness and the boy was arrested within 24 hours. He later agreed to withdraw his statement and his parents offered an apology too.

TAMIL NADU VS SUHAS KATTI

Case of obscene, defamatory and annoying message about a divorcee in the yahoo message group.

E-Mails were also forwarded to the victim from a false e-mail in the name of the victim. Annoying phone calls flooded believing that she solicited sexual relationship.

Accused was her family friend. Interested in marrying her. Her marriage with another ended in divorce. His proposal was refused.

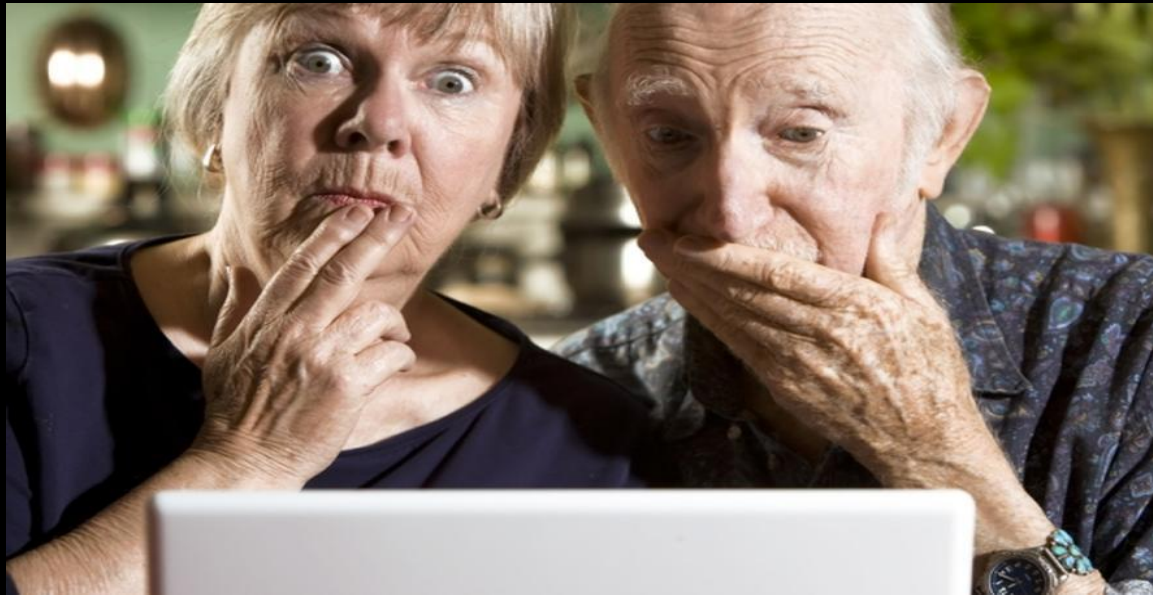
Convicted under sections 469, 509 IPC and 67 of IT Act 2000 First case of conviction under IT Act. (2+1+2 yrs of Imp concurrent. Rs 500 x 2 fine imposed. Nov 4, 2005, Judge Arulraj, Addl Chief Metro Mag, Egmore.

PORNOGRAPHY
SEC 67 A



.XXX ????

- The Internet Corporation for Assigned Names and Numbers ([ICANN](#)) has given the .XXX top-level domain (TLD) its final approval in March, 2011. The TLD is meant to give pornographic websites a clearly marked place/home on the Internet.
- Nine ICANN board members voted in favor of .XXX, while three members opposed and four abstained. Some countries expressed shock over this development.



SEC 67 A
2008 AMENDMENT

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.

➤ **Watching a porn movie in private is not an offence**

**66E. PUNISHMENT FOR VIOLATION OF
PRIVACY. (INSERTED VIDE ITA 2008)**

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;

KARNATAKA ASSEMBLY???
MINISTERS ???



Triple-ex-ministers?



Amul
Never adult-rated

The three ministers, Laxman Savadi, C C Patil and J Krishna Palemar, caught on camera viewing obscene clips on the floor of Karnataka legislative Assembly could face jail and one of them even a non-bailable arrest-warrant. As the law stands today Mr. Savadi and Patil **can be booked under Section 292 of IPC for public exhibition, etc.**, of an obscene object. The third minister J Krishna Palemar, who was in possession of the mobile phone, could face a non-bailable warrant if a complaint is registered against him. Palemar can be convicted with **imprisonment up to five years and penalty up to Rs 5 lakh under IT Act**

What is Objectionable?

Obscenity and pornography

Richard A. Spinello observes, Internet its remarkable growth "is not without its social costs".



SHOULD WE

NO:

- **Ronald Dworkin** says that no conduct should be suppressed by law unless it can be shown to harm some one without any persuasive evidence of the causal influence.
- **John Stuart Mill** felt that we do not know in advance what social, moral, or intellectual developments will turn out to be possible, necessary or desirable for human beings and for their future and **free expression** intellectual and artistic something which may need to be fostered and protected as well as merely permitted is essential to **human development as a process** which does not merely happen but so far as possible is rationally understood.
- Since human beings are not just subject to their history but aspire to be conscious of it the development of human individuals, of society and of humanity in general is a process itself properly constitutes in part by **free expression and the exchange of human communication**.



**CANADIAN SUPREME COURT CASE OF *R V BUTLER*, [1992] 1 SCR THE
452 (*BUTLER*)**

The Women's Legal Education and Action Fund (**LEAF**), argued that pornography was an issue of sex discrimination which caused systemic gender inequality and the subordination of women within society.

Verdict: there was a 'causal relationship between obscenity and the risk of harm to society at large' and that 'the relationship between pornography and harm was sufficient to justify Parliament's intervention

PUBLISHING CYBER PORNOGRAPHY (SUMMARY)

Actions covered Publishing

Penalty First offence:

Subsequent offence:

Relevant authority

Appeal lies to

Investigation Authorities

**transmitting cyber pornography
causing to be published**

**Simple or rigorous imprisonment
up to 5 years and fine up to Rs 1
lakh**

**Simple or rigorous imprisonment up
to 10 years and fine up to Rs 2 lakh**

Court of Session

High Court

1. Controller of Certifying Authorities (CCA)
2. Person authorised by CCA
3. Police Officer not below the rank of Deputy Superintendent

CHILD PORNOGRAPHY

Child pornography is identified as a heinous crime that may operate as a gate to further crimes, like sex tourism and sexual abuse, aside from being a record of a sexual assault on a child

There is a steady rise in the number of child pornography cases registered and arrests in India. According to minister of state for home M Ramachandran as told to Lok Sabha, across India, the number of cases stood at 99 in 2007, 105 in 2008 and 139 in 2009

study conducted on child abuse by the Ministry of Women and Child Development, 30.22% of children surveyed reported they had been exposed to dirty pictures.

INTERPOL has **cited Germany** as one of the major producers of child pornography, with the Netherlands and the United Kingdom as the major distribution centres. United States is one of the largest markets of demand for child pornography

Ninety-four of 187 [Interpol](#) member states had laws specifically addressing child pornography as of 2008

67B (2008) amendment

IN UK

- In the United Kingdom, the Obscene Publications Act, 1959 was amended by the Criminal Justice and Public Order Act of 1994 (CJPOA) to deal with the specific problem of internet pornography by extending the Act to cover the transmission of electronically stored data. It makes service providers liable for material placed on the internet by a third party thus requiring them to monitor material for obscene matter.
- Further the Protection of Children Act, 1978 was amended by CJPOA, 1994 to include photographs in electronic data format.



CYBER TERRORISM AND CYBER WARFARE

66 F: CYBER TERRORISM

INDIA – VICTIM OF CYBER WARFARE

- In early March, 2013 suspected Chinese hackers breached the computers of India's top military organisation, **the Defence Research and Development Organisation (DRDO)**, in what was touted to be amongst the biggest such security breaches in the country's history. Defence Minister A.K. Antony ordered a probe.
- Hackers from Algeria also carried out an attack on websites run by the DRDO, the Prime Minister's Office and various other government departments last year. A group called 'Pakistan Cyber Army' had also hacked into several Indian websites.
- According to CERT-In (the Indian Computer Emergency Response Team), which is a government-mandated information technology security organization, an estimated 14,392 websites in the country were hacked in 2012 (till October).

STUXNET

- ```

C:\>dir
Volume in drive C: is FREEDOS_C95
FreeSpace version 0.82 pl 3 XMS_Swap [Dec 16 1987]

C:\>dir
Volume in drive C: is FREEDOS_C95
Serial Number is 64F-95B
Directory of C:\

DIRS DIRS 08-25-84 6:23
DIRS 35 08-25-84 6:24
DIRS 512 8-25-84 6:23
DIRS 93,963 08-26-84 6:24
DIRS 881 08-26-84 6:24
DIRS 512 08-26-84 6:24
DIRS 45,815 04-17-84 9:19

File(s) 6 file(s) 142,838 bytes
Dir(s) 1 dir(s) 1,064,517,632 bytes

```

**DEFINITION**  
**SEC 66 F: IT ACT ( 2008**  
**AMENDMENT ACT)**

Cyber terrorism, with an intention to threaten integrity or security of nation denying access to computer source, or penetrating into, or introducing computer contaminant, (B) exceeding the authority to access or unauthorizedly access to the restricted data **with an intention to threaten security, sovereignty etc.** imp for life.



## DEFINITIONS

- **Dorothy Denning** defines cyber terrorism as "the convergence of terrorism and cyberspace. It is understood to mean unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in the furtherance of political or social objectives".
- **Mark Pollit** defines cyber terrorism as a "premeditated, politically motivated attack against information, computer systems, computer programmes, and data which result in violence against noncombatant targets **by** sub national groups or clandestine agents".

## INTERNATIONAL COOPERATION

- The Convention on Cyber Crime (**ETS no 185**) ("**ECCC**"), **2001 at Budapest** is the first international treaty addressing crimes committed via the Internet and other computer networks.
- Articles **2-6** which address offences against the confidentiality, integrity and availability of computer data and systems, may be used to address the offence of cyber terrorism.
- South Africa is the only African country to sign the European Convention on Cyber crime (**ECCC**).



## LEGISLATIONS ON CYBER TERRORISM

The United States of America introduced the Patriot Act of 2001 in response to the 9/11 attacks.

South Africa :legislations on cyber terrorism and terrorist financing- 1. the Prevention of Organised Crime Act 38 of 1999 ("POCA"),  
2. the Financial Intelligence Centre Act 38 of 2001 ("FIGA"),  
3. the Electronic Communications and Transactions Act 25 of 2002 ("ECT"),  
4. Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004 ("PCDTRA").



# USA, PATRIOT ACT, UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM.

The Act has eased restrictions on electronic surveillance to facilitate the capture of terrorists.

contains anti-money laundering provisions in order to prevent terrorists from achieving any financial gain from their actions.

includes terrorism and computer crimes on its list of offences.

However, the Act has been criticized for violating the civil rights of ordinary American citizens.



## SOUTH AFRICA

Cell phones have also been used to track terrorists and to provide evidence against them. South Africa has introduced the Regulation of Interception of Communication Act 2002 (RICA) for this purpose.



## UK

- The Terrorism Act of 2000 was introduced to address terror attacks in the United Kingdom. The listed prohibited actions include endangering another person's life or creating a serious risk to the public health or safety, acts designed to seriously interfere with or disrupt an electronic system and acts involving serious violence to or death to another person or serious property damage.
- Section 1(2)(e) of the Terrorism Act 2000 describes a terrorist act as one that "is designed seriously to interfere with or seriously disrupt an electronic system".
- On 14th December 2001, the British Anti-Terrorism, Crime and Security Act
- the United Kingdom government is seeking protective measures against the cyber terrorist threat. IT HAS SET UP National Technical Assistance Centre which is a surveillance advice and interception facility

## THE USES OF INTERNET: COMMUNICATION



## DEAD DROPS AND STEGANOGRAPHY

An extremely creative way devised by terrorists of using the internet is of dead drops. Dead drops are traditionally associated with the world of espionage as depictive of exchange of information without the two parties actually ever having to meet. This way there is never any evidence of there being a conspiracy. Internet dead drops go a step further by also erasing the very information which is exchanged. After creating free email accounts the information is saved in an email draft without being sent, later the other participant is given the adequate account details and accesses the draft.

Another way in which terrorists use the internet is one which is even more veiled and concealed below the layers. This way is of steganography though which information is hidden in different media so it is not visible to others apart from the intended recipient.<sup>^</sup>

<sup>^</sup>See, Hummel, M. 2008. Internet terrorism. *Homeland Security Rev.*, 2 p. 117 - 130

## INDIA IS AT SPECIAL RISK

The International Monetary Fund has pointed out how India is at a especially huge risk of being home to terrorist financing

India is a member of the multi-national Financial Action Task Force (FATF), an inter-governmental organization founded in 1989 by the G7 which was created to develop policies to counter terror financing and this very Task Force has questioned India's efficacy in the same domain.<sup>^</sup>

Section 17 of the Unlawful Activities (Prevention) Act makes raising funds an offence where there is likelihood that they will be used for terrorist acts.

<sup>^</sup>'Indian laws cannot counter terror-funding'. 2010. *The Indian Express*, [online] July 18th. Available at: <http://www.indianexpress.com/news/indian-laws-cannot-counter-terrorfunding/648241/> [Accessed: 30 Sep 2013].

## INTERNET AND CYBER- TERRORISM

- Cyber terrorism is defined, however for the use of the internet by terrorists there has not been the coinage of either a term or a definition.
- The use of internet is made by terrorists for
  - perpetrating psychological warfare
  - for recruitment
  - for financial support for networking
  - for planning
- The use of internet by terrorists can be said to be the biggest contributing factor for the success of many terrorist attacks
- This is widely acknowledged but very less concrete action has been taken very less concrete action on and this is where this paper finds its launching platform.

## 66F. PUNISHMENT FOR CYBER TERRORISM

(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 authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized 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 authorized 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 26

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(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life’.

**69 POWERS TO ISSUE DIRECTIONS FOR INTERCEPTION OR MONITORING OR  
DECRYPTION OF ANY INFORMATION THROUGH ANY COMPUTER RESOURCE  
(SUBSTITUTED VIDE ITAA 2006)**

- (1) Where the central Government or a State Government or any of its officer specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense 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 transmitted received or stored through any computer resource.
- (2) The Central Government shall prescribe safeguards subject to which such interception or monitoring or decryption may be made or done, as the case may be.
- 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 which has been directed under sub section (1), extend all facilities and technical assistance to -

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

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

□ (c) provide information contained 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 an imprisonment for a term which may extend to seven years and shall also be liable to fine

## **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, defense 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-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by 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 also be liable to fine.

## SEC 69 B. 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 authorised 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 sub-section (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

# THE INDIAN JOURNEY

## Information Technology Act of 2000

### Indian Computer Emergency Response Team (CERT-In), 2003

Section 66 F of the Act deals exclusively with cyber terrorism and punishes those who 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” carry out denial of service attacks, attempt to penetrate a computer source without authorization or introducing any computer contaminants. And it is likely to cause death, destruction of property, damage, or disruption of supplies and services.

Section 84B makes abetment an offence

Section 84C makes attempt to commit an offence also punishable

Information without authorization knowing that it might be used to damage the security of the State, lead to defamation, or incitement to an offence. The punishment

Section 69 of the IT Act deals with interception, monitoring and decryption of information. It empowers the Controller to direct any agency or government to intercept any information or communication through any computer resource if he is expedient to do so in the interest of sovereignty of the state.

It gives directions to the telecommunications service providers to

use prescribed security measures for detailed checks and balances on the

websites VOIP encryption and Real Time Information Sharing agency and also has tie ups with international bodies.

# CYBER DEFAMATION

**66 A:**

## DEFAMATION – CYBER DEFAMATION

- The term defamation is used to define the injury that is caused to the **reputation** of a person in the eyes of a third person. The injury can be done by words oral or written, or by signs or by visible representations. The intention of the person making the defamatory statement must be **to lower the reputation** of the person against whom the statement has been made in the eyes of the general public.
- Cyber defamation is **publishing of defamatory** material against another person **with the help of computers or internet**. If someone publishes some defamatory statement about some other person on a website or send emails containing defamatory material to other persons with the intention to defame the other person about whom the statement has been made would amount to cyber defamation

## LAW ON CYBER DEFAMATION

- The Section 66A of the Information Act, 2000 does not specifically deal with the offence of cyber defamation but it makes punishable the act of sending grossly offensive material for causing insult, injury or criminal intimidation.
- Section 66A of the IT Act says that any person who sends, by means of a computer resource or a communication device:-
  - any information that is **grossly offensive** or has menacing character; or
  - any content information which he **knows to be false**, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,
  - any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

## JUDICIAL RESPONSE TO CYBER DEFAMATION

- ❖ In the first case of cyber defamation in India, SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra (CS(OS) No. 1279/2001, Delhi High Court), the reputation of a corporate was being defamed by an employee of the plaintiff company by sending derogatory, defamatory, obscene, emails obscene, vulgar, filthy and abusive emails to its employers and also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director. The Hon'ble Judge of the Delhi High Court passed an ex-prate ad interim injunction observing that a prima facie case had been made out by the plaintiff.

The Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.

**ART OF LIVING CASE**  
**VYAKTI VIKAS KENDRA, INDIA PUBLIC CHARITABLE TRUST THR**  
**TRUSTEE MAHESH GUPTA & ORS VS. JITENDER BAGGA & ANR.3**  
**(CS(OS) NO. 1340/2012 )**

The four plaintiffs in this case filed a suit against the defendants for damages and permanent injunction, mainly on the ground that they are aggrieved and hurt because of certain highly defamatory materials posted on [www.blogger.com](http://www.blogger.com), owned by Google (defendant No.2) by Mr. Jitender Bagga (defendant No.1). As per the plaintiff, the defendant No.1 was indiscriminately sending e-mails and publishing a large number of blog posts, which according to them was making highly vulgar, disgusting and abusive references towards His Holiness Sri Sri. Ravi Shankar, owner of Art of Living Foundation, and other persons associated with the Art of Living.

Delhi High Court held Google to be an “intermediary” within the definition of Section 2(1)(w) and Section 79 of the Information Technology Act, 2000. t under Section 79(3)(b) of the IT Act, 2000, Google is under an obligation to remove unlawful content if it receives actual notice from the affected party of any illegal content being circulated/published through its service. Google is also bound to comply with Information Technology (Intermediaries Guidelines) Rules 2011.



## CYBER DEFAMATION

Crime of Defamation

Online: Sec 66A

IPC s 499

Both a crime and a civil wrong.

## TATA SONS VS. TURTLE INTERNATIONAL

The Delhi High Court has held that publication is a comprehensive term, embracing all forms and mediums “ including the Internet. That an internet publication has wider viewership, or a degree of permanence, and greater accessibility, than other fixed (as opposed to intangible) mediums of expression does not alter the essential part, i.e. that it is a forum or medium. There is much sense to have more defined criteria taking into account the nature of the internet content. Injunctions on internet content should not be readily granted (especially ex-parte) since, firstly the internet is an easy, self publishing platform providing a medium of expression for marginal individuals not having corporatist outlets. Secondly, the internet facilitates the distribution of content for a minor cost to a vast audience. Both the alleged injury and the free speech concern are greater due to the wider dissemination of the content.

## AUTHORITY TO INTERCEPT

69. Authority to intercept, monitor, decrypt, etc.

69A Power to block public access to any information of system

69B Power to monitor, collect, traffic data or information through any computer source for cyber security: Intermediary or in charge of information is under obligation.



## OFFENCES

- Preservation of information by intermediary, if not 3yrs plus fine, 67C
- Breach of directions of Controller or Certifying authority, 2 yrs plus one lakh s 68
- Disclosure of information by intermediary or any person who has access, in breach of lawful contract, 3 yr 5 lakh S 72A.
- Attempt to commit offences, half of longest term + fine 84C

**REGULATORY AUTHORITIES  
COMPUTER EMERGENCY  
RESPONSE TEAM ( CERT-IND)**

## RELATED PROVISIONS

- Section 67C asks intermediaries to preserve and retain certain records for a stated period.
- Section 69B is also quite stringent to intermediaries.
- Section 69A has been introduced to enable blocking of websites by the central government.
- Section 69B provides powers to central government to collect traffic data from any computer resource. It could be either in transit or in storage. This amendment was necessary for security purpose but it may lead to abuse of power by government.
- Section 72A has been introduced to cover offences regarding disclosure of information in breach of lawful contract. Section 80 empowers inspectors instead of D.S.P's to enter, search, etc.

- 
-

## REGULATORY AUTHORITIES

- ✓ COMPUTER EMERGENCY RESPONSE TEAM ( CERT-IND)
- ✓ Sec. 70 A: Nodal Agency: Computer Emergency Response Team-In , 70B National Agency for incident response
- ✓ **POWERS**
  - ✓ 70 Power to declare any system as Critical Information infrastructure, to protect
  - ✓ Working since 2004
  - ✓ Instructs DOT to block websites
  - ✓ Collection, analysis and dissemination of information on cyber incidents
  - ✓ Forecast and alerts of cyber security incidents
  - ✓ Emergency measures for handling cyber security incidents
  - ✓ Coordination of cyber incident response activities
  - ✓ Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents

# **INTERMEDIARIES**

# AVNISH BAJAJ

## BAAZEE.COM



## FACTS

- Avnish Bajaj, CEO of Baazee.com, an online auction website, was arrested for distributing cyber pornography.
- A video clip was offered for sale, shot on a mobile phone of two children of a school in delhi indulging in an explicitly sexual act. The managing director was prosecuted under sec 292 and sec 67 of the IT Act. He contended that bazee.com is only a service provider and provides a platform and when it has come to his notice it was withdrawn immediately.
- Baazee.com India Private Limited ('BIPL'), a wholly owned subsidiary of Ebay Inc. USA, and the owner of the website <http://www.baazee.com>, was during the relevant period in the process of being acquired by and consequently renamed as Ebay India Private Limited (EIPL). BIPL had its main office at Mumbai and another office in Delhi. During November to December 2004 the petitioner Avnish Bajaj was the MD of BIPL (which later was renamed as EIPL).

The website [baazee.com](http://baazee.com) provided an online platform or market. I have read the User agreement carefully - I am above 18 years of age. I have read and agreed to abide by the [baazee.com](http://baazee.com) user agreement...." The next stage in the registering process was reached after the person clicked on "Accept Terms & Submit". Thereafter an email was sent to the person by [baazee.com](http://baazee.com) in which a link was provided for activating the account. A person who registered following the above online procedure could either sell or buy products on the electronic market that [baazee.com](http://baazee.com) offered by using the [baazee.com](http://baazee.com) ID and password where a seller and a buyer could interact.

## CONTD.,

- Ravi Raj, a fourth year student of the Indian Institute of Technology (IIT) Kharagpur, was registered as a seller with [baazee.com](http://baazee.com) since 21st July 2004. He had already been using the site for listing products for sale. His email ID was [psell@sify.com](mailto:psell@sify.com).
- In the evening of **Saturday 27th November 2004**, Ravi Raj placed on the [baazee.com](http://baazee.com) website a listing offering an MMS video clip for sale at Rs. 125 per piece.
- He adopted the seller's name as Alice Electronics and gave his address as 12-A/39, Roshpa Tower, Main Road, Malanche, Kharagpur. In order to avoid detection by the filters installed by [baazee.com](http://baazee.com), Ravi Raj included the clip under the category Books and Magazines and sub-category 'e-books'.
- **(Filters)** Although [baazee.com](http://baazee.com) did have a filter for some of the words which appear on the website, the listing nevertheless took place. For instance, the word "sex" at Seriall No. 23 of the list and word "sexual" at Seriall No. 70 of the list were definitely part of the suspected words.

- the item description on its site: "**Item 27877408 - DPS Girls having fun!!! full video + Baazee points.**"
- DPS Girls having fun!!! Do you want to see that video clip which has rocked the whole DELHI and now has become a hot point of discussion in the entire Nation?
- YES, Then what are you waiting for!!!!
- Just order for this product and it will be delivered to you within few hours.
- This video is of a girl of DPS RK PURAM which has been filmed by his boyfriend in very sexual explicit conditions.
- Please note: This video clip of around 2:30 Minutes and will be send to you as an email attachment.

## CONTD,

- At around 8.20 pm on Saturday 27th November 2004 information was received on email from Amit Vohra using emailed [threadsincp@sify.com](mailto:threadsincp@sify.com) for Community Watch. The mail titled "fraud report about item ID 27877408" read as under:
- **User's Message:**
- The username of the party is alice-elec. This person is trying to sell a video which is illegal in India as it was shot on two people who are below the legal age of 18 & pornography is illegal in India. You need to sort this issue & you should even report it to the legal authorities as this can get your site in trouble.
- . This email was assigned to Namrata of BIPL at around 8.25pm on 27th November 2004 itself. At around 6:25pm on the next date i.e. 28th November 2004, which happened to be a Sunday, it was assigned to Swapna Sawant of the BIPL and the priority was shifted to the 'high alert' category.
- The video clip was removed on 29th November 2004 Monday at around 10:38 am. Meanwhile eight persons with distinct IDs located in different parts of the country including Calcutta, Nellore, Pune, Delhi, Bangalore and Chennai had purchased it.

## THE INFORMATION TECHNOLOGY (INTERMEDIARIES' GUIDELINES) RULES, 2011 ('THE INTERMEDIARY GUIDELINES')

were notified in April, 2011 as rules enacted in exercise of powers conferred under section 87(2)(zg) read **with Section 79 of** the Information Technology Act, 2000 (as amended) ('**the IT Act**')



## **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.

## **XII. INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES (SUBSTITUTED VIDE ITA-2006)**

### **79 Exemption from liability of intermediary in certain cases**

(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. (corrected vide ITAA 2008)

(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 (Inserted Vide ITAA 2008)

(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 (ITAA 2008)

(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.

Explanation:- For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

## DUE DILIGENCE RULES -2011

- *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; ( copy right infringement)
  - (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;

## CONTD...,

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**;

(f) deceives or misleads the addressee about the origin of such messages or **communicates any information which is grossly offensive or menacing in nature**;

(g) 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

## EXCEPTIONS TO LIABILITY

- (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;

## DUTIES OF INTERMEDIARIES

1. after being brought to the knowledge of the intermediary about the objectionable content hosted or posted on the website he shall act within six hours and disable such information
2. he shall preserve such information and associated records for at least 90 days. the intermediary is having the right to terminate the access or usage to the computer source in case of violation of agreement or privacy policy.



- 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.

Intermediary shall give assistance to government agencies in matters of investigation and 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.

# **ADJUDICATING AUTHORITIES**

## CYBER APPELLATE TRIBUNAL [S 57]

- ✓ **Cyber regulations Appellate Tribunal** is established by the Central Government. The Central Government shall specify the matters and places in relation to which the tribunal may exercise jurisdiction.
  - ✓ The tribunal comprises of a Presiding officer to be appointed vide a notification by the Central Government.
  - ✓ An appeal shall lie to this Tribunal against any decision/order of the Controller of Certifying Authorities or any other certifying authorities. Any person aggrieved by the order of this Tribunal may prefer an appeal to the High Court within 60 days from the date of communication of the order of the Tribunal.
- 
- An appeal from an order made by Controller or an adjudicating officer under this Act lies to Cyber Appellate Tribunal having jurisdiction in the matter.
  - However, no appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.
  - Every appeal shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received
    - Endeavour shall be made to dispose off the appeal finally within six months from the date of receipt of the appeal.

# **OFFENCES COMMITTED OUTSIDE INDIA**

## EXTENSION OF IPC

- Any person liable by any Indian Law, to be tried for offence committed beyond India shall be dealt with under IPC, in the same manner as if such act had been committed in India. (Section 3)
- IPC applies to any offence committed by any citizen of India in any place without and beyond India; any person on any ship or aircraft registered in India wherever he may be.



## CRIMES OUTSIDE INDIA

Section 75 of the IT Act clearly lays down that its provisions shall also apply to "any offence or contravention committed outside India by any person, irrespective of his nationality", provided that such act involves a computer, a computer system or computer network located in India.



## STATE'S ARM EXTENDS

- Attorney General of Minnesota sought to regulate online gambling by asserting that a state will have jurisdiction over any cyber issue since accessing a webpage is as good as 'bringing' the site into the territorial jurisdiction of the state in which it is viewed. The Minnesota Attorney General's Office distributed a Warning to All Internet Users and Providers, available at <http://www.state.mn.us/cbranch/ag/memo/txt> (visited 26/03/2008).

# STATE VS. MOHD. AFZAL AND OTHERS

2003VIIAD(DELHI)1,,

2003(3)JCC1669

- Digital evidence played an important role in this case. Computerized cell phone call logs were heavily relied upon in this case.
- A laptop, several smart media storage disks and devices were recovered from a truck intercepted at Srinagar pursuant to information given by two of the suspects. These articles were deposited in the police “malkhana” on 16th December, 2001. Although the laptop was deposited in the “malkhana” on 16th December, some files were written onto the laptop on 21st December

- Evidence found on the laptop included:
- 1. fake identity cards,
- 2. video files containing clippings of political leaders with Parliament in background shot from TV news channels,
- 3. scanned images of front and rear of a genuine identity card,
- 4. image file of design of Ministry of Home Affairs car sticker,
- 5. the game 'wolf pack' with the user name 'Ashiq'. Ashiq was the name in one of the fake identity cards used by the terrorists.



## ISSUES RAISED BY THE PROSECUTION

- 2. Analysis of the Windows registry files of the suspect laptop showed that its hard disk had not been changed.
- 3. If internet has been accessed through a computer then the actual date of such access would be reflected. Additionally, if any change is made to the date setting of the computer, it would be reflected in the history i.e. in the REG file.
- 4. A hard disc cannot be changed without it being reflected in the history maintained in the REG file.
- 5. It was not possible to alter the date of any particular file unless the system date had been altered.
- 6. The files written on the laptop on 21st December were “self generating and self written” system files. These were created automatically by the laptop’s operating system when the laptop was accessed by law enforcement agencies at the “malkhana”.

- **Issues raised by the Defence:** Although the laptop was deposited in the Government “malkhana” on 16th December, some files were written on the laptop on 21st December. The date setting on a computer can be edited.
- 4. In the absence of verified time setting and reliable information about the hard disc being original, there is
- no certainty that the material found on a later date, was exactly the material, which may have existed on a previous date.
- 5. Hard disc is a replaceable component and could be formatted. If a hard disc was replaced, it would not contain the data which was stored earlier unless it was re-fed.
- 6. The Windows registry files can be edited.

- 7. The back up of complete suspect hard disc was not taken by the law enforcement agencies.
- 8. The date setting on a file is related to the date setting on the computer. It is possible to modify this date.
- 9. Information stored in a computer is on a magnetic medium which can easily be polarized. Therefore, any data in a computer can be changed by a knowledgeable person.
- 10. The date of last access to a file is treated differently by different software. The time of last access was meaningless in the absence of knowledge as to what software is used to process the file.
- 11. Software which was installed in a computer could be modified and un-installed without leaving any trace.

# MINISTRY OF HOME AFFAIRS

This is to certify that this car belongs to the ministry of home affairs, and this is the property of India. No body allows to stop this car. India is a very bad country and we hate India. We want to destroy India and with the grace of God we will do it. God is with us and we will try our best. This ediet wajpiee and Advani we will kill them. They have killed many innocent people and they are very bad persons and their brother Bush he is also a very bad person he will be next target he is also the killer of innocent people he has to die and we will do it. Ministry of home affairs Government of India.

## QUESTIONS DEFENCE RAISED (IN P-ATTACK CASE)

- CAN THE HARD DISK OF A COMPUTER CHANGED ?
- CAN THE CLOCK OF A COMPUTER CHANGED ?
- WHY A BACK-UP OF HARD DISK WAS NOT TAKEN?
- TIME STAMPS ?

## BLOCKING

- Section 69A grants powers to the Central Government to "issue directions for blocking of public access to any information through any computer resource". In English, that would mean that it allows the government to block any website. While necessity or expediency in terms of certain restricted interests are specified, no guidelines have been specified. Those guidelines, per s.69A(2), "shall be such as may be prescribed". It has to be ensured that they are prescribed first, before any powers of censorship are granted to any body.

## CONTD.,

- While earlier, under section 69, the Controller had powers to order decryption for certain purposes and order 'subscribers' to aid in doing so (with a sentence of up to seven years upon non-compliance), now the government may even call upon intermediaries to help it with decryption (s.69(3)). Additionally, s.118 of the Indian Penal Code has been amended to recognize the use of encryption as a possible means of concealment of a 'design to commit [an] offence punishable with death or imprisonment for life'.

**PROPERTY OFFENCES  
– IN –  
CYBER SPACE**

**66 B PUNISHMENT FOR DISHONESTLY RECEIVING STOLEN  
COMPUTER RESOURCE OR COMMUNICATION DEVICE  
(INSERTED VIDE ITA 2008)**

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both

**66C PUNISHMENT FOR IDENTITY  
THEFT. (INSERTED VIDE ITA 2008)**

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

## FRAUD AND CYBER FRAUD

### Fraud

415 to 420 IPC

S 25 what is fraudulently

Intention to deceive

Actual or possible injury

### Cyber fraud

Spam emails

Email frauds

Online investment newsletters

Nigerian fraud



The Delhi High Court :  
"phishing".

- The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, they could use for purposes of head-hunting, the defendants composed and sent e-mails to third parties in the name of NASSCOM.
- The plaintiff had filed the suit inter alia praying for a decree of permanent injunction restraining the defendants from circulating fraudulent e-mails purportedly originating from the plaintiff. The court declared "phishing" on the Internet to be a form of Internet fraud and hence, an illegal act.
- This case had a unique bend since it was filed not by the one who was cheated but by the organization who was being wrongly represented that is NASSCOM. The court held the act of phishing as passing off and tarnishing the plaintiff's image

## MISCHIEF

### Mischief 425 to 440 IPC

Intention to cause wrongful loss

Act causing destruction of  
property

### Section 43 of IT

Program manipulation

Output manipulation

Data alteration

Computer vandalism

## FORGERY – ELECTRONIC FORGERY

- “ *A person is guilty of forgery if he makes a false instrument with the intension that he or another shall use it to induce somebody to accept it as genuine*” .
- Chris Reed and John Angel “Computer Law” 4<sup>th</sup> Ed, Blackstone Press p. 281
- Computer forgery - criminal gets access to data kept on a computer and alters it making computers as targets for criminal acts.
- IPC 464 amended to include electronic forgery.
- 29 A defined it.

## **ELECTRONIC FORGERY**

Section 463 of the IPC (after amendment) defines forgery, in relation to the electronic record, as making any false electronic record or part thereof with an intent to cause damage or injury to the public or to any person, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed.

## **COMPUTER FORGERY IN AP TAX CASE**

Rs. 22 Crore was recovered from the house of the owner of a plastic firm by the sleuths of vigilance department,  
Generated 6000 vouchers to legitimize the amount recovered,  
Made after the raids were conducted .  
Fake computerized vouchers

## THEFT – CYBER THEFT

- Physical theft, possession of property shifts from owner
- S 378: Intends to take dishonestly any movable property out of possession of any person, without consent moves that property. (s22 corporeal property, not attached s moveable property)
- Cyber theft – no complete shifting of possession of property from owner
- Data theft (s 2 ‘data’)
- S 43 Data theft – illegally copied, or taken without knowledge.
- Data is intangible so not movable property, data stored in a medium (CD pen-drive computer) medium is property so covered by IPC.

## DATA IS PROPERTY

- HSBC – customer credit card info was passed on, which led to Rs. 1.8 crore scam.
- ACME Telepower Pvt Ltd. Patented Product Power Interface Unit, valued 750 crore, an employee leaked to rival Lambda Eastern Telecom ltd, ACME shifted its 10 million R&D unit to Australia.
- Abhinav Guptha v State of Haryana, 2008 CrLJ 4536, JCB India's employee resigned on a condition that he would not join a rival company. He was uploading the data, drawings of JCB. Data, trade secrets was stolen, amounts to hacking, anticipatory bail rejected.

## THEFT ON HIGH SCALE

- Criminals hacked the data base of Card system solutions and took up to 200,000 visa, MasterCard and American Express credit cards.
- High tech companies in Israel where alleged to have planted surveillance software on computers of their business rivals.
- In 2004 the United Kingdom lost approximately 3 billion pounds due to unauthorised access to computer systems, data threat, virus attacks and financial frauds. See: Nuurrie weekly newspaper <http://www.nuurrie.com/section.asp?section=10> ( accessed on 26-03-08)

## CYBER EXTORTION

- Vijay R Ninawe of Abu Dhabhi received lewd cyber content from Rita Basu, and Ruchira etc.
- Cyber love developed with Rita. She mailed 'will die if you don't marry'. VR stopped mailing.
- Ruchira Sengupta continued mailing and informed that Rita committed suicide & police booked case
- Some mails from high court & police.
- Ruchira told him that they need to fight litigation with lawyers help, He deposited 96 lakh.
- Vijay Came Mumbai, lodged complaint.



**CONTD.,**

No woman, no suicide.

Pranab Mitra who generated all mails, arrested. He is 51 year old former manager of Gujarat Ambuja Cement company, started internet love and made money to land in jail.

June, 13, 2003 TOI

## CHEATING

Online fraud and cheating are some of the most lucrative businesses that are growing today in the cyber space. Credit card crimes, contractual crimes, offering jobs, prizes etc

(R.v. Preddy (1996) 3 ALL ER 481- traditional criminal concepts should not be applied to online fraud or any other form of intangible information)

**66D PUNISHMENT FOR CHEATING BY PERSONATION BY USING COMPUTER  
RESOURCE  
(INSERTED VIDE ITA 2008)**

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

## KOLA MOHAN'S CYBER LOTTERY FRAUD

- Kola Mohan (AP) created website & email 'eurolottery@usa.net.' showing him as beneficiary of 12.5 million pound in Euro lottery.
- After confirmation of email address, a telugu newspaper published this as news. Using this, he gathered huge sums from the public as well as from some banks.
- Fraud came to light when a cheque for Rs 1.73 million discounted by him with Andhra bank got dishonored.



## SPOOFING

- Electronic impersonation is colloquially called spoofing, which can be used in furtherance of variety of cyber crimes
- Technologies of anonymity further complicate the task of identifying a suspect
- Fraudsters escape by means of 'looping' or 'weaving' through multiple sites in a variety of nations.

## CONCLUSION

- Prevention and punishment of crime is responsibility of the state.
- There should be uniform criminal law to curb these crimes in the whole of the world.
- Law has to recognize electronic documents, transactions and accept them in the court of law
- Further investigation to secure the identity of the cyber criminals, so that the state agencies can detect, prosecute and punish.



