Enclosure to Item No. 4 (14/6)

UNIVERSITY OF MUMBAI

Post Graduate Diploma Course in Cyber Laws.

Ordinances, Regulations, Scheme of Papers and syllabus for the Post Graduate Diploma Course in Cyber Laws.

Introduced from the academic year 2005-2006

Paper I : - Jurisprudence, Information & Cyberspace Technology

Introduction:

1. Emergence of Cyberspace – From pages of Science-fiction.
2. Defining Cyber space.
3. Evolution of Computer Technology & Cyber law – A time line
4. Governance of Internet & other relevant details outlined.

Cyber Ethics

5. A look at evolving ethics in information age with special reference to free music, flash mobs and Pune BPO's case.

A glance at the Technology as an enabler.

We would provide concrete concepts as grounding for beginners and gradually introduce the questions and ideas that are abstract and future oriented.

6. A brief historical perspective, non-technical overview of computer/mobile devices and the internet. Both hardware and software concepts are quickly introduced as a foundation step.

.....3/-

7. A glance of computer/mobile applications as they are used in the cyber space, automating and increasing workforce's productivity and mobility.
8. The world of network from the very basic LAN and WAN to a global infrastructure- the evolving internet.
9. Risks and ethical issues are uncovered along with a quick look at how applications are shaped exploring the process and the problems in software creation embedding artificial intelligence.
10. The impact of cyber space on society especially social behaviour, governance, learning & education, health care and business including entertainment.

Information Technology Act, 2000

11. Overview of IT Act 2000 along with rules with relevant sections and rules highlighted along with amendments to other laws.

A conceptual overview along with laws/rules relating to the following:

12. Cryptography including a discussion on algorithms & public/private key encryption.
13. Digital Signatures –concept & their legal recognition.-
14. Electronic Governance (E – Governance)
15. Legal Recognition of Electronic Records
16. Certifying Authorities
17. Network Service Providers Liability

Access to the cyberspace

18. Access to the Cyber Space would deal with copper wires, co-axial cables and wireless networks as a means of communication to the cyber space. How the telecom, cable/broadcast and other spectrum policies affect the market mechanisms influencing the net citizens' ability to use it.

Jurisprudence

19. Jurisprudence: A case digest with 125 to 150 typical cases, sets a present context in different categories of legal issues.

An emerging framework for international governance of cyberspace.

20. Here we briefly focus on initiatives of internet policy making at international levels by individual inter-governmental organizations, which are considerable feats, pointing to an emerging international framework. As an illustrative example of policy making, we could discuss the TRIPP Agreement and the WTO, ICAAN and UNICITRAL in the area of Intellectual Property, Domain Names and model e-commerce law.

Paper II : - E – Commerce & Issues

Contextualizing E- Commerce

1. Case study of various portals / web sites with a view to survey what they are doing in an attempt to showcase the essence of the Cyberspace. The latest trend for additional features incorporating mobile applications/solutions based on evolving/existing technologies like RFID, GPS/GPRS, SMS based and others.
   Generating a profile of the legal concern, issues and vulnerabilities.
   Some recommended sites in typical categories could include Yahoo!, Rediff, Google, Overture, Amazon, Nielsen, America on line, itunes, Times of India – e-paper, Slashdot, Chemconnect, Netflix, ebay, Orbitz, Fruste, Verisign, Encase, Doubleclick, WIPO, ICAAN and PayPal.

A suggested Framework for evaluation:

They could be evaluated giving a brief introduction, how it can be navigated in the cyber space, its design, web analytics, business models, digital market addressed, digital automations, auction and dynamic pricing, conflicts with other brick channels, trusted transactions, security, data privacy, intellectual property, governance responsibilities, ethics adhered to and other relevant benchmarks.

2. ***A Legal dimension:***
This could be followed by a check-list/and a more detailed discussion on legal concerns & issues based on a few above case studies or a consolidated hypothetical case addressing:

e-business plan with a patenting opportunities / liabilities, jurisdiction issues, intellectual property rights addressed and managed, internet privacy, consent of third party/parties, information security and non-contractual liability like torts, internet taxation, on-line contract formation, internet payment system, regulatory issues, information security check-list, terms and conditions of use, adherence to commercial transaction facilitating laws (like UCiTA), employment issues, email and internet usage check-list, internet advertising policies, web site intellectual property audit, insurance policies and online dispute resolution.

3. ***E Commerce- Salient Features,***
comparing/contrasting with other e-models especially the e-governance, e-healthcare and e-learning.

4. ***Some focus issues:***
   - **Jurisdiction** and zoning
   - **Online contracts** – Contrasting/comparing click wrap agreements with others.
   - **Privacy Issues** and along with a discussion on protection of personal data.
   - **Torts** in cyber space along with negligence, strict liability, immunities and privileges
   - **Security and evidence** in e-commerce with respect to digital signatures, encryption and digital certificates.
   - **Taxation Issues** in Cyber spaces - Taxes related to the Internet (e-commerce), tax evasion and the problems of taxation on the net, International taxation, US & European views

.....6/-

- **Anti-trust cases** along with emerging checks on the market place with open source, co-evolution. interoperability and standards becoming the order of the day instead of competition.
- **Converging business models** for service with information appliances like iPods.

5. **E- banking**: An illustrative example in Indian Scenario.

Legal issues related to e-banking (internet banking) and use credit/debit cards on the net like buying Indian railway or cinema tickets.

Or e-Securities could be considered instead/additionally.

Paper III: - IPR Issues in Cyber Space & beyond IPR.

Contextualizing the content issues:

1. Case Studies:

(a) Relating to digital media especially relating to Napster & its subsequent generation variants bring out how Copyright, Contract and Technology Shape the Business of Digital Media.

[b] A landmark case relating to Patents - State Street Bank Case

[c] Domain Names cases addressed by different forums like WIPO, a High Court and others in the past.

2. Intellectual Properties: a brief overview with regards to cyberspace.

....7/-

Copyrights

3. Copyright a law that assigns and delineates the borders of rights in information. Many in society believe that it has exceeded its benefit as an incentive of people to create, investing the effort and time in original and innovative intellectual works – This discussion would give an overview as well as focus on relevant issues that the law addresses, including subject matter concepts of "originality" & "fixation"; their entitlements, infringements and limitations; limited time period highlighted by the Sonny Bono case.
4. Other than copyright would examine alternatives including data protection, contract law, encryption, open source and a tax/royalty system.

Patents:

5. Patents: This would address the recent development in intellectual property laws to patent computer software and business methods. Applications in patent offices of US, Europe and Japan only indicate a popular paradigm shift. The business method patents such as Amazon.com's one click purchasing and Priceline.com reverse auction are illustrative. The present legislative attempt to narrow the ability to patent new business processes is looked at along with India's position on these issues.

Domain Names:

6. Trademarks and Domain name- A collision in Cyber Space. A review of attempts to address the Domain name disputes worldwide by many regimes along with investigating different mechanisms that attempted to solve the scarcity along with Online Dispute Resolution Policy.

Database Protections:

7. Databases: Protection with respect to US, European & Indian Laws.

Some Other issues:

8. Software- Copyright or Patent?

9. Linking, framing, meta tags, robots & search engines-a brief discussion.

10. Digital right management and anti-circumvention laws. Is contract & digital rights management are two alternatives or together additional ways to protect content? Evaluate.

Paper IV: - Cyber Crimes, Digital forensics & Evidence

Contextualising digital Crimes

1. Understanding Cyber Crimes – A sample of at least 25/30 cases in different categories, encompassing crimes against or/and supported by the computer and the network. This raises concern about

- Unauthorised access
- Web Spoofing
- Hacking and web defacement
- Denial of Service Attacks
- Malicious Code
- Financial Crimes – including online fraud, counterfeiting etc.
- Social Engineering Attacks
- Password Cracking
- Steganography
- Identity theft
- Cyber stalking
- Pornography
- Harassment
- Murder and death threats
- Gambling
- Spamming
- Sale of controlled items – tobacco, wines etc.
- Commercial espionage
- Commercial extortion
- Data manipulation

- Software/hardware piracy
- Money laundering
- Threat or disruptions to health and safety, shut-down of essential services and extortions.
- Espionage and Terrorism
- Others including the ones involving mobile devices.

These acts add to the challenges faced by law enforcement bodies to deal with.

2. A case study of a real life hacking focusing on the anatomy of a hack, with clear outline of the objective, the methodology, the techniques & tools deployed at each stage of the process.
3. A live demo of system penetration by an ethical hacker, to get a context of what it means to hack, along with its venerability report and a corresponding look at the response of an intrusion detection system.
4. Profiling the need to combat Digital Crime by State Enforcement as well as comparing/contrasting cyber crimes with conventional crimes

Rules & Procedures

5. Information Technology Act- Penalties & offences, investigations and adjudication.
6. Indian Penal Law – An overview with relevant sections/rules highlighted.
7. Criminal Procedure code - An overview with relevant sections/rules highlighted.
8. Evidence Act - An overview with relevant sections/rules highlighted.

Critical Evaluation of Rules & Procedures

9. Are these enough /more to address digital crimes? Are there more challenges?

- *A critical evaluation by participants who can work out the ideal model rules and procedures.*
- *Identify areas not covered by IT Act and classify those addressed by other laws and issues that await attention*

Focus on some other typical issues:

10. Obscenity & Pornography on the Internet
11. Freedom of Speech & Expression
-Defamation & Hate Speech included.

Precautions undertaken by corporate & individuals – voluntarily as well as under regulations

Voluntarily as a corporate/individual policy

12. Adherence of Standards/Specifications. A very brief outline discussion on BS7799, CC, CDSA, FIPS Pub, GMITS, ITIDF, OSI Security, Security Information Object, GSS-API, Kerberos, PEM, PGP, PKCS, S-HTTP, S/MIME, SOCKS, SSL, NIST publications..

13. Security as understood and defined in present context as well as defining/profiling the perceived/real threat.

14. Understanding the business needs for security.

15. Align IT Infrastructure

16. Risk Assessment

17. IT Controls: their identification and design.

18. Implementation

19. Feedback in the form of measure, monitor and report.

20. A quick look at concept/products of/for Intrusion detection, firewalls, Anti Virus solutions, Security scans, continuous process of updating & configuration (example patches released by Microsoft)

Some of these standards/specifications/processes could be a part of the regulatory requirements mentioned below.

.....11/-

As a Regulatory requirement

21. Under the following Act very briefly outline identifying a regulatory requirement:
Information Technology Act 2000 (as already covered earlier), Sarbanes-Oxley Act, Gramm-Leach-Bliley Act (GLBA), Committee of Sponsoring Organisation (COSO), Control Objectives for Information and related Technology (COBIT), Health Insurance Portability & Accountability Act (HIPAA) and others as they evolve.

Incident occurs, what next

22. An internal corporate policy in place for incident response/ individual's desire. An evaluation.

Reporting the incident on desire of victim

23. A FIR and in few cases a remand order.
24. Other process including how the accused with a different profile needs to be handled than normal criminals, accessing their motives, degree of empathy, sympathy & anger expressed based on the nature of crime, age of the accused & degree of offence to be considered

Investigating the crime scene by first responders

25. An overview of enforcement response to digital evidence, nature of digital evidence and the forensic process.
26. Introduction
27. Electronic devices with their potential evidence profile.
28. Investigative Tools & Equipments
29. Securing the Scene & its Evaluation.
30. Documenting the Scene
31. Evidence Collection
32. Packaging, Transportation and storage of Evidence collected.

Precautions in the investigation/examination of digital evidence.

33. A brief summary as to the special precautions to be taken to document, collect, preserve and examine the fragile natured evidence, with due diligence. Fragile, as it can be altered, damaged or destroyed by improper handling or examination loosing evidence value.

Investigative uses of technology and Forensic Examination of Digital Evidence.

34. Introduction to Digital Forensic as they pose challenges for its admissibility in court. Proper procedures / process need to be in place which may include collection, acquisition/imaging, examination, assessments, analysis, documenting and reporting. Recognised forensic tools usage is recommended in the process, as is the case world wide. Forensic examination could address peculiar issues in each crime category. Also the understanding of anti forensic tools would help.

This would very briefly bring out, to the extent possible, (as digital forensics skill set neatly meshes with the skills required in order to respond to security incidents, as earlier profiled in the case study - point 2/3) the following issues:

- Digital Forensics using with open source tools-a few demos.
- An overview summary of Computer Crime, as already provided earlier.
- Preparation of sterile examination media
- Acquisition, collection and seizure of digital/magnetic media.
- Recovering deleted data from a smart/cell phone /digital camera/PDA's
- Documenting a "Chain of Custody"
- Understanding Microsoft Windows from a forensics point of view
- Working with NTFS
- Combing Partition table and boot record
- Investigating The Master File Table (MFT)

- Linux/Unix forensics –a brief note
- Investigating data streams
- Dates and times of file storage
- File deletion/recovery
- Internet Usage Data/Swap Files/Temporary Files/Cache Files – how recovered?
- Safe handling of original media and preservation thereof.
- Original media copies in bitstream
- Rootkits & other techniques commonly used for data hiding
- CD-ROM media examination
- Carving out files "hidden" in unallocated/slack disk space
- Password cracking
- Presentation of data in court –Issues to be addressed-see below
- The evidence marking, storage and transmittal.
- Use tools such as Paraben/Encase Forensic Edition, X-Ways Forensic Addition, Forensic TookKit (FTK) and others.

,Recreating digital crimes Scene

34. Recreating the crime scene.

Creation of digital evidence by the forensic unit

36. A brief summary of the details including the chain of custody – physical item & data acquisition, the preliminary handling of digital evidence (pre law enforcement), the acquisition and examination processes.

Courtroom presentation of digital evidence

37. A brief summary covering the 'Search and Seizure Issues', ' Integrity, Discovery and Disclosure of Digital Evidence', ' Courtroom Preparation and Evidence Rules' and 'Presentation of Digital Evidence'.

Courtroom Presentation and Evidence Rule would focus on the preliminary considerations for the prosecutor when reviewing the scope of the investigation to date, effective pre-trial communication between prosecutor, investigator and forensic examiners and also evidentiary issues like authentication and hearsay in digital evidence context.

Presentation of Digital Evidence would include educating the audience, what needs to be proved/disproved?, Expert witness/scientific method evidence, recurring issues in computer crime trials with respect to identity, knowledge, chronology of events, Jury instructions, jury selection, presenting complicated technical issues.

Paper V : - Practical Training:

Contemporary Issues debated.

Contemporary issues debated with a view to help individual participants to develop an independent opinion on issues.

Partial list of issues that could be considered:

- Cyber cafés how they are regulated all over the world and India.
- ISP's responsibility to block unwanted sites – a law.
- Spamming, is it a crime?
- Spyware compared and contrasted with other similar technologies that put privacy at stake.
- Instant messaging logs as admissible evidence
- Gambling, online gambling and lottery tickets compared/ contrasted.
- Can BPO's in India succeed in creating a data base of their employees?
- Digital right management and music video piracy with the arrival of broadband in India.
- How the handhelds, PDA's and smart phones change the landscape of cyber laws?
- Ad-hoc networks like Bluetooth, infra red and Wi-Fi challenge the digital evidence.
- Trojan Horse defence – a discussion
- Cloning a mobile phone – is it a forgery?
- Rights of employees in the cyber age – How much can the employer monitor employees at work.
- Is blog equivalent to press, implications, if any?
- India an outsourcing capital – a critical legal view as to what needs to be done to realize the potential.
- Taxation issues on downloads of music, video of software.

.....15/-

Hands on/ Demos/ Presentations

E-mail header reading to identify the source.
Understanding the use & how Logs are read.
An introduction to Biometrics.
Understanding the role of ISP's

A Demo: Mobile Sim Card cloning & some related technologies.

Understanding a few top Security tools deployed.

Basic understanding of how penetration testing or ethical hacking is undertaken

Understanding a few forensic/ anti forensic tools.

A Case Study of challenges- as posted by investigative & forensic experts demonstrating their use of forensic tools.

Developing writing/presentation skills for court room's presentations. This is with a view to developing individual's ability to put together, a clear bigger picture, effectively using digital evidence.

Moot Court – Putting skills to test.

Some Independent Presentations:

- The open source – A Presentation
- A NASSCOM Presentations on Security as well as a view on the Industry.
- A ISACA Presentation on Security Policies & the certifications they offer.

....16/-

Preferred Technology Orientation Courses but Are Optional.

(These courses are being offered by few specialised institutions & universities.)

For beginner, intermediate and advanced learners.

For a security perspective:
For understanding the technology for security/ethical hacking tools:

Computer Languages: Advanced C and Assembler under DOS, Windows
Ethernet Programmes: Sniffer, ARP, TCP/IP Connect Programme.
Protocols: TCP/IP, ICMP, UDP
Network Programmes: Raw-Sockets, HTTP Client/Server programme, Trace Route, Syn flood, Shell code, Root kits
Windows Internals: Buffer Overflow, PE File Format, Sql Injection, Mobile Sim Cards programming.
Tools: Network Monitor, NC, Ethereal, SNORT, Debugger, NMAP, NESSUS.
System penetration testing demo using the above tools.

For digital forensic perspective:
One must have a comprehensive understanding of the subject from definitions to data recovery techniques to uncover the methods used in cyber-attacks.
It would briefly include the basic concept of digital forensic, data recovery, digital evidence collection, reconstructing past events, deterrence through attacker's ID, destruction of trace and email uncovered, digital footprint and criminal tracking, the individual exposed, possibility of terrorist attack and the cyber underground world.

A brief understanding of how everything is tied up, located and utilized as digital evidence as it exists on computer hard disks, mobile/electronic devices, shared network or embedded systems.

Tools used for collecting and analyzing digital evidence along with their strengths and limitations.

Putting to test all our perspectives:
Case studies describing the actual digital crimes committed and how subsequently investigated.

.....17/-

For those looking for a deeper technical understanding, details of network and data communications could of interest.

This would include networks and networking essential, networking fundamentals, LAN and WAN, clients and servers, peer to peer, the network medium, network software, network services, network types, network design basics-network design, designing a network layout, standard topologies; Hubs, switches. Variations of the major topologies, constructing a network layout: Networking media: Networking cabling: Tangible physical media, primary cable types, Network Interface Cards (NIC), choosing network adaptors for best performance, special purpose NICs, wireless adapters, remote boot adapters, Driver Software OSI and 802 Networking models.

Advanced Understanding would include Network Communications and Protocols-Function of Packets in Network Communications: Protocols: Common Protocols-Transmission Control Protocol/Internet Protocol (TCP/IP), IP Addressing: NetBIOS and NetBEUI, IPX/SPX, Putting Data on the Cable: Channel Access Methods, Function of Access Methods, Major Access Methods, Choosing an Access Method.

Enterprise and Distributed Networks: Modems in Network Communications, Carriers, Remote Access Networking: Creating Larger Networks; Repeaters, Bridges, Routers, Gateways, Switches.

Wide Area and Large-Scale Networks; Advanced WAN Technologies; X.25; ISDN (Integrated Services Digital Network); Frame Relay; ATM (Asynchronous Transfer Mode); FDDI (Fibber Distributed Data Interface); SONET (Synchronous Optical Network); SMDS (Switched Multi megabit Data Service).

The Internet: A World-Wide Resource, What is on the Internet? Domain Name System (DNS), Making an Internet Connection, Dial-Up Connections, Digital Connection Types, Connection Considerations.

****