Indian Cyber Laws..!!

- Laws are Silent in time of War

Presented by

Dr. M. Prasad, M.Tech, Ph.D, MISTE, MCSI, MIAENG,
Professor & Head,
CSE Department,
B V C I T S, Amalapuram
Overview

- Cyber Crime?
- Cyber Law?
- Need / Importance of Cyber Law for India in Present Era
- Cyber Law Deals with…???
- Indian Cyber Laws
  - IT Act-2000 & Some Sections
  - IT Act Amendment-2008 & Features
- References
"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".

Cyber Crime?

- Any crime with the help of computer and telecommunication technology.
- Any crime where either the computer is used as an object or subject.
Cyber Law?

- Cyber Law is the law governing cyber space.
- Cyber space includes computers, networks, software's, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.
Need / Importance of Cyber Law for India in Present Era

- Cyber crime in India resulted in 29.9 million people being victim of cybercrime involving direct financial losses to the tune of $4 billion and $3.6 billion in terms of time spent in resolving the crime.
- 4 out of 5 online adults (80%) being victim of cyber crime
- 17% of adults online experiencing on their mobile phones

(source: Norton Cybercrime Report)
The main reasons for India as a main target of cyber crime are:

- Rapidly growing online user base (121 million internet users, 65 million active internet users, up 28% from 51 million in 2010).
- 50 million users shop online on ecommerce and online shopping sites.
- 46+ million social network users.
- 400 million mobile users had subscribed to data packages.

(source IAMAI 2011).
Need / Importance of Cyber Law

- Internet has dramatically changed the way we think, the way we govern, the way we do commerce and the way we perceive ourselves.
- Information technology is encompassing all walks of life all over the world.
- Cyber space creates moral, civil and criminal wrongs.
- It has now given a new way to express criminal tendencies.
Most people are using email, cell phones and SMS messages for communication.

Even in "non-cyber crime" cases, important evidence is found in computers /cell phones.

Ex. In cases of divorce, murder, kidnapping, organized crime, terrorist operations, counterfeit currency etc.

Since it touches all the aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace therefore Cyber Law is extremely important.
Cyberspace is open to participation by all

“IT” has brought Transition from paper to paperless world

The laws of real world cannot be interpreted in the light of emerging cyberspace to include all aspects relating to different activities in cyberspace

Internet requires an enabling and supportive legal infrastructure in tune with the times
Cyber Law Deals with

- Cyber Crimes
- Electronic or Digital Signatures
- Intellectual Property
- Data Protection and Privacy
Categories of Cyber Crime

- Cybercrimes against persons.
- Cybercrimes against property.
- Cybercrimes against government.
Cybercrimes against *persons*.

- Cyber stalking
- Impersonation
- Loss of Privacy
- Transmission of Obscene Material.
- Harassment with the use of computer.
Cybercrimes against property

- Unauthorized Computer Trespassing
- Computer vandalism
- Transmission of harmful programmes
- Siphoning of funds from financial institutions
- Stealing secret information & data
- Copy Right
Cybercrimes against government

- Hacking of Government websites
- Cyber Extortion
- Cyber Terrorism
- Computer Viruses
Some Other Crimes

- Logic Bombs
- Spamming
- Virus, worms, Trojan Horse
- E-Mail Bombing
- E-Mail abuse etc.
The Information Technology Act, 2000 (IT Act), came into force on 17 October 2000.

The primary purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

Information Technology Act 2000 consisted of 94 sections segregated into 13 chapters.
## Important Cyber Law Provisions in India

<table>
<thead>
<tr>
<th>Offence</th>
<th>Section under IT Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tampering with Computer source documents</td>
<td>Sec.43</td>
</tr>
<tr>
<td>(with out the permission of in charge)</td>
<td></td>
</tr>
<tr>
<td>Hacking with Computer systems, Data alteration</td>
<td>Sec.66</td>
</tr>
<tr>
<td>Publishing obscene information</td>
<td>Sec.67</td>
</tr>
<tr>
<td>Un-authorized access to protected system</td>
<td>Sec.70</td>
</tr>
<tr>
<td>Breach of Confidentiality and Privacy</td>
<td>Sec.72</td>
</tr>
<tr>
<td>Publishing false digital signature certificates</td>
<td>Sec.73</td>
</tr>
</tbody>
</table>
Section 43

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

- Access, download, Copy any data from such computer
- Introduces Computer Virus into any computer.
- Damages any computer network or computer.
- Changes Account Settings.

**Punishment**

- He shall be liable to pay damages by the way of compensation not exceeding 1 Crore to affected person.
Hacking with Computer System

- Information residing in a computer resources must be either:
  - Destroyed
  - Deleted
  - Altered
  - Diminished in value or utility
  - Affected Injuriously

Punishment

3 yrs. Or Fine up to 2 lakh.
Section 67

- Publication or transmitted in the electronic form any material which contains *sexually explicit acts or conduct*.

**Punishment**

- 1\textsuperscript{st} conviction with 2 to 5 years of imprisonment and fine of 1 lakh rupees.
- 2\textsuperscript{nd} or subsequent conviction with the imprisonment up to 7-10 years and also with fine which may extend to 10 lakh rupees.
Some other Sections

- **Section 65**: Tampering with computer source document.
  
  **Punishments:**
  
  Offences are punishable with imprisonment up to 3 yrs and/or fine up to Rs. 2 lakh.

- **Section 69**: Interception, monitoring of any information regarding the integrity, Security or defense of India, friendly relations with foreign countries.
  
  **Punishment:**
  
  2 lakh and /or jail not extending 5 yrs

- **Section 72**: Violation of the privacy policy
  
  **Punishment:**
  
  Fine up to 5 lakh and jail not extending 2 yrs.
**IT Act-2000 Sections – Contd.**

Crimes under Indian Penal Code and Special Laws

<table>
<thead>
<tr>
<th>Offence</th>
<th>Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sending threatening &amp; Defamatory messages by email</td>
<td>Sec 503 &amp; 499 IPC</td>
</tr>
<tr>
<td>Forgery of Electronic records</td>
<td>Sec 463 IPC</td>
</tr>
<tr>
<td>Bogus websites, cyber frauds</td>
<td>Sec 420 IPC</td>
</tr>
<tr>
<td>Email spoofing &amp; Abuse</td>
<td>Sec 463 &amp; 500 IPC</td>
</tr>
<tr>
<td>Web-Jacking</td>
<td>Sec 383 IPC</td>
</tr>
<tr>
<td>Online sale of Drugs</td>
<td>NDPS Act</td>
</tr>
<tr>
<td>Online sale of Arms</td>
<td>Arms Act</td>
</tr>
</tbody>
</table>
Some other Sections

- **Section 502A**: Publishing, Transmitting images of the private area of a person without his or her consent.
  
  **Punishment**: 2yrs./2 lakh.

- **Section 419A**: Cheating by any communication device or computer resource
  
  **Punishment**: 5yrs.

- **Section 417A**: Identity Theft
  
  **Punishment**: 2yrs.
IT Act Amendment-2008

- The Information Technology Amendment Act, 2008 (IT Act 2008) has been passed by the parliament on 23rd December 2008.

- It received the assent of President of India on 5th February, 2009.

- The IT Act 2008 has been notified on October 27, 2009.
IT Act Amendment-2008 – Cont.

- ITA-2008, is a new version of IT Act 2000.
- Provides additional focus on Information Security.
- Added several new sections on offences including Cyber Terrorism and Data Protection.
- 124 sections and 14 chapters.
- Schedule I and II have been replaced & Schedules III and IV are deleted.
Digital signature has been replaced with Electronic signature.

Section 67 of the old Act is amended.

Sections 66A to 66F prescribe punishment for obscene electronic message transmissions & cyber terrorism.

Amended section 69 gives power to the state.

Sections 69 A and B, grant power to the state to direct blocking for public access of any information through any computer resource.
World & Cyber laws

- The Great firewall of China monitors every movement in cyber space and protect to publish any offensive content.

- China have a hold on every content which is harmful or dangerous for the government of China.

- Brazil is considered world’s biggest airport for Hackers.

- Iran is also a dangerous country for the Netizens. He also have a Crime Police unit for crime in Cyber Space.
References

- www.cyberlawclinic.org/
- http://cyberlawsindia.net/
- http://mit.gov.in/hindi/node/1435#
- http://slideshare.net
- http://inextlive.jagran.com/What-is-SOPA--201201180029
- http://www.ahyep.com
- www.leawo.com/free-powerpoint-templates/
- http://www.ncrb.nic.in