INDIAN LEGAL RESPONSE TO CYBER SECURITY

A PRESENTATION

BY

PAVAN DUGGAL,

ADVOCATE - SUPREME COURT OF INDIA

PRESIDENT , CYBERLAWS.NET

PRESIDENT , CYBERLAW ASIA

CHAIRMAN - ASSOCHAM CYBERLAW COMMITTEE

INDIA COMMITTED TO CYBER SECURITY

- Recent Fibre Optic intrusion case
- Mumbai Attacks
- Bangalore , Delhi bomb attacks
- Terrorist attacks on the rise
- Cyber security is a focus area of the Government
- Law is dedicated to preserving the veracity of computers and data resident therein.

IT ACT AMENDMENTS

- Information Technology Amendment Act, 2008
- Passed by both the houses of Parliament in end December, 2008
- Published in the Official Gazette on 5th February, 2009
- Rules being framed under the amended law

COMMUNICATION DEVICES

- Law dedicated to the use of computers, computer systems, computer networks and computer resources.
- All communication devices now specifically brought within the ambit of the Indian Information Technology Act, 2000
- "Communication Device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image;

CYBER SECURITY DEFINED

- "Cyber security" means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction; {Section 2 (nb) }

SECURITY PROCEDURES

- The Central Government may for the purposes of sections 14 and 15 of the IT Act, 2000 prescribe the security procedures and practices.
- Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

SENSITIVE PERSONAL DATA

- Sensitive Personal Data and information brought within the ambit of special protection of the Indian IT law.
- Protection of sensitive personal data in a computer resource made the mandatory responsibility of its possessor, dealer or handler
- Negligence in this regard leads to statutory damages exposure

STATUTORY DAMAGES

- Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected. {Section 43 A}

STATUTORY DAMAGES (contd.)

- "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities

REASONABLE SECURITY PRACTICES AND PROCEDURES

- "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

SENSITIVE PERSONAL DATA

- "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

STOLEN COMPUTER RESOURCE / COMMUNICATION DEVICE

- 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 INR 100,000/- or with both.{Section 66 B}

CYBER TERRORISM

- INDIA IS POSSIBLY ONE OF THE VERY FEW COUNTRIES THAT HAVE ADDRESSED THE ISSUE OF CYBER TERRORISM LEGALLY.
- CYBER TERRORISM HAS BEEN DEFINED AS A HEINOUS OFFENCE UNDER THE AMENDED IT ACT, 2000 {Section 66 F}
- ONE OF THE WIDEST POSSIBLE KNOWN DEFINITIONS OF CYBER TERRORISM INCORPORATED UNDER INDIAN IT LAW

CYBER TERRORISM- DEFINED

- Whoever,-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 –
- denying or cause the denial of access to any person authorized to access computer resource; or

CYBER TERRORISM DEFINED (contd.)

- Attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or
- Introducing or causing to introduce any Computer Contaminant.

CYBER TERRORISM DEFINED (contd.)

- 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

CYBER TERRORISM DEFINED (contd.)

- 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

CYBER TERRORISM PUNISHMENT

- security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,
- commits the offence of cyber terrorism.
- Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life ' .

INDIAN CYBER SECURITY AGENCY

- 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. {Section 69 B}

INTERMEDIARIES DEFINED

- "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes. {Section 2 (1) (w)}

INTERMEDIARIES & CYBER SECURITY

- Inherent role of Intermediaries in cyber security recognized.
- Their responsibility for third party data is recognized under the law.
- They have been straddled with the mandatory obligation to do due diligence , while discharging their obligations under the IT Act, 2000
- Non compliance with law ensures legal exposure, both civil and criminal, for the intermediaries.

DATA PRESERVATION

- 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.
- 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. {Section 67 C}

TRAFFIC DATA DEFINED

- "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information. {Section 69 B}

TRAFFIC DATA ACCESS

- The Intermediary or any person in-charge of the Computer resource shall when called upon by the authorized agency, 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. {Section 69 B}

MONITORING & COLLECTION

- The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
- Draft rules being finalized in this regard
- Any intermediary who intentionally or knowingly contravenes the provisions of Section 69B (2), shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

PROTECTED SYSTEM

- The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.
- "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which , shall have debilitating impact on national security, economy, public health or safety. {Section 70 (1)}

CERT-IN

- The Indian Computer Emergency Response Team has been designated to serve as the national agency for performing the following functions in the area of Cyber Security,-
- collection, analysis and dissemination of information on cyber incidents
- forecast and alerts of cyber security incidents

CERT-IN(contd.)

- Emergency measures for handling cyber security incidents
- Coordination of cyber incidents response activities
- Issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed {Section 70 B (4)}

CYBER SECURITY IMPLEMENTATION

- For carrying out the provisions of the amended IT Act, 2000 CERT-IN may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person {Section 70 B (6) }

FAILURE TO PROVIDE INFORMATION

- Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction of CERT-IN , shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to INR 100,000/- or with both. {Section 70 B (7) }

NEW CHALLENGES

- SOCIAL NETWORKING
- P2P
- USER GENERATED CONTENT
- MISUSE OF VOIP
- SPYWARE AND MALWARE

CONCLUSION

- India has come up with a comprehensive legal approach to Cyber Security
- Appropriate secondary legislation is currently being finalized
- Need of the hour is the effective and stringent implementation of the law
- Existing law and policies on Cyber Security need to be constantly reviewed and strengthened.
- The Indian legal approach to Cyber Security is a great example for other countries to follow in Asia Pacific and the rest of the world.