CYBERLAW - EXISTING CYBER LEGAL ISSUES, REGIMES & CHALLENGES
A PRESENTATION
BY
PAVAN DUGGAL
ADVOCATE, SUPREME COURT OF INDIA
PRESIDENT, CYBERLAWS.NET
PRESIDENT, CYBERLAW ASIA
HEAD, PAVAN DUGGAL ASSOCIATES
CYBERLAW – EXISTING CYBER LEGAL ISSUES, REGIMES & CHALLENGES

- Twitter posts land 2 Saudi men in prison-sentenced for 10 and 8 years respectively
- Twitter posts expose adguru to 2 litigations for crores of damages
- Different jurisdictions similar cyber legal regimes
For the First Time, Hackers Have Used a Refrigerator to Attack Businesses

Security researchers at Proofpoint have uncovered the very first wide-scale hack that involved television sets and at least one refrigerator.

Yes, a fridge.

This is being hailed as the first home appliance "botnet" and the first
The world that we are currently living is a different world altogether and it promises to become even more different, difficult and complex as days go by.
Today in 2014, Internet is not only our lifeline but also the foundation for a large number of human activities and endeavors.

It is ironic that founding fathers of the Internet had no inkling that Internet could be used for various criminal purposes or could have legal ramifications.

However today, almost 2 decades after the advent of the World Wide Web, Cyberlaw and cybercrime are important subjects for consideration by all stakeholders in the digital and mobile ecosystem.
9/11 & 26/11 ATTACKS

© of images belongs to the respective copyright holders
NSA REVELATIONS

© of images belongs to the respective copyright holders
NSA PROOF INTERNET

© of images belongs to the respective copyright holders
Today, world is concerned about the security and sovereignty of its computer resources and computer networks.

Countries do not want powers outside the territorial boundaries to listen to their communications or access their data that is running on their domestic networks.

It is only natural to expect countries start looking in direction establishing country specific internets.
IMPORTANT CASES

- Agricultural equipment manufacturing company data theft case
- Offensive emails to company matter
- Phone defects blog case
- Twitter rumour defamation case
IMPORTANT CASES

- Twitter fake handles used against company case
- True Caller and CEO phone number compromise case
- Calls for fake interviews on social media case
- Gurgaon call centre spy camera girl termination case
CYBER BULLYING GALORE

© of images belongs to the respective copyright holders
VIRTUAL LOLITA & 103 INDIANS

© of images belongs to the respective copyright holders
Facebook and Twitter were used to disseminate hateful content leading to the Bangalore Cyber terror attacks.
15TH AUGUST, 2012 - BANGALORE MASS MIGRATIONS

© of images belongs to the respective copyright holders
3rd December 2010 - CBI official website hacked by Pakistan Cyber Army
Lot of threatening language put up on the hacked main page of CBI website
Case registered under Section 43 and 66 of the IT Act, 2000
DR. L. PRAKASH- INDIA’S FIRST LIFE TIMER CYBER CRIMINAL

© of images belongs to the respective copyright holders
RECENT HACKING

- EMAIL ACCOUNTS OF SENSITIVE INSTITUTIONS AND DEPARTMENTS OFFICIALS HACKED

- ACCOUNTS BELONGED TO NATIONAL DEFENCE ACADEMY & DRDO OFFICIALS
IMPORTANT CASES

- ARIF AZIM CASE
- BAAZEE.COM CASE
CYBERCRIME AS A SERVICE

Pune-based global hacker Amit Tiwari arrested

Engineering dropout Amit Vikram Tiwari, 32, compromises 950 foreign email accounts and 171 Indian; he was nabbed in 2003 as well.
DATA PROTECTION

- The issues relating to confidential information and data of corporate and their adequate protection have not been adequately addressed.

- The said law is not a comprehensive law on data protection or on digital secrets. Having a couple of sections on Data protection does not serve the requirements of corporate India.
Further the concept of privacy in India needs to be substantially enhanced strength and further developed. The law passed has used very basic concepts of personal privacy.

The needs to be further well developed to incorporate therein issues pertaining to personal as well as data privacy. Further the entire issue pertaining to privacy has not been appropriately addressed; both data privacy and personal privacy are issues that require adequate attention.

The Department of Personnel & Training, Government of India is coming up with a new legislation on data protection. However, lots of work needs to be done in this regard.
INTERMEDIARY

© of images belongs to the respective copyright holders
"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.
INTERMEDIARIES AND DUE DILIGENCE UNDER THE IT ACT, 2000

- Intermediaries are required to do due diligence under the terms of the amended Information Technology Act, 2000.
- This due diligence must be done to ensure compliance with the relevant parameters of the amended Information Technology Act, 2000.
Liabilities of Intermediaries and the Indian Cyberlaw

- Liability of intermediaries has been specifically now provided under Section 79 of the amended Information Technology Act, 2000.

- “Google v/s Vishakha” case before the Hon'ble Supreme Court of India.

- The emphasis on exercise of due diligence by intermediaries is an important aspect. However, enforceability and implementation of the Information Technology Act, 2000 has always been a challenge.

- Most of the companies in India comply with the Information Technology Act, 2000 in breach rather than in observance.
LIABILITIES OF INTERMEDIARIES AND THE INDIAN CYBERLAW

- There could have exposure to legal consequences, both civil and criminal, for the company and its top management.

- Civil liability-damages by way of compensation upto 50 million INR per contravention.

- Criminal Consequences - The top management could also be exposed to criminal consequences ranging from imprisonment of 3 years to life imprisonment and fine from 1 Lakh INR to 10 Lakhs INR.
LIABILITIES OF INTERMEDIARIES AND THE INDIAN CYBERLAW – CRIMINAL CONSEQUENCES

© of images belongs to the respective copyright holders
NEED FOR DUE DILIGENCE

- Reasonable Prudence ensues compliance with the requirements of law, that being Indian Cyberlaws, IT Act, IT Rules, notifications, bye-laws and circulars made thereunder.
COMPLIANCES BY PAVAN DUGGAL ASSOCIATES

- Pavan Duggal Associates -role in helping companies ensure compliances with the Indian Cyberlaw and rules thereunder.

- Pavan Duggal Associates assist all intermediaries to ensure documented due diligence under the Information Technology Act, 2000.
Asia Pacific Legal 500 says about Pavan Duggal Associates:

“Cyberlaw specialist Pavan Duggal Associates Advocates is the first port of call for many in terms of cases involving data theft, usually companies that have experienced theft of confidential or commercially sensitive information by former employees.”

“Pavan Duggal Associates Advocates provides niche expertise in cyber law.”
Indian Cyberlaw has created the appropriate legal framework for promoting e-commerce in the country as was giving legality to electronic format. The said lead framework has provided for various enabling provisions that provide for electronic authentication and cyber security related issues.

All legal entities have a duty to ensure that its business operations needs to comply with the parameters of Information Technology Act, 2000 as also rules and regulations made thereunder.
ONLINE MONITORING, INTERCEPTION, BLOCKING & SURVEILLANCE

© of images belongs to the respective copyright holders
ONLINE MONITORING, INTERCEPTION, BLOCKING & SURVEILLANCE

- Issue of interplay between the online sovereignty of nations vis-à-vis activities of monitoring, interception and surveillance in cyberspace.

- Questions like where would the online sovereignty of nations begin and end are important issues which require appropriate consideration. The paramount issue is the surveillance. A society where, not just the Government but also service providers and intermediaries are in one way or the other carrying out various surveillance activities.

- The governments of the world want to know what we are talking, publishing, transmitting, generating, uploading, hosting on our computer resources, computer networks or communication devices. - Re Turkey new Internet law.
With Surveillance emerging as a popular undertaking of the governments, it will be important to watch how individual liberties, rights and obligations get appropriately balanced when seen on the scale of national sovereignty, integrity and security.
RIGHT TO BE FORGOTTEN

© of images belongs to the respective copyright holders
Cyber crime is increasingly jumping on to the mobile bandwagon.

The huge advent of malware and smart phones once again puts into focus the entire issue of mobile crimes.

As mobile crimes continue to grow, the relevant stakeholders will increasingly call upon governments of the world to effectively strengthen their cyber-legal regimes to cover and regulate the newly emerging mobile threats and mobile crimes.
CYBER SECURITY
CYBER TERRORISM

© of images belongs to the respective copyright holders
There is a huge possibility of cyber terrorism and high profile attacks on Critical Information Infrastructure and related companies.

The corporate focus on cyber security will shift from the concern about the loss of personally identifiable information to concern about cyber vandalism, hacktivism and theft of trade secrets.
Data privacy concerns are already sky rocketing that is why data privacy will continue to be an important issue.
BRING YOUR OWN DEVICE (BYOD)
BRING YOUR OWN DEVICE (BYOD)

- The advent of Bring Your Own Device (BYOD) has changed the landscape.
- However, the security, confidentiality and veracity of data are important legal challenges that will have to be appropriately addressed by cyber legal regimes in order to enable large and mass scale adoption of BYOD.
CLOUD COMPUTING
CLOUD COMPUTING

- Regulation in cloud computing would be seen as positive and logical way forward as they grappled with privacy and security on the cloud.
BIG DATA

- Google likely to know more about your spouse than you do.
- Big data is already an integral part of our lives and its use for data analytics purposes brings forward various legal policy issues.
- Further, organizations need to verify that the sources they intend to use have appropriate permissions from the users who provide the data to perform any additional analytical activities.
The advent and adoption of data analytics at a mass scale requires that appropriate attention is given to legal issues concerning big data like authenticity, veracity of data, data collection, data archiving, data retention, jurisdiction, privacy, confidentiality and other data collection related issues as the world moves forward.
VIRTUAL CURRENCIES

© of images belongs to the respective copyright holders
VIRTUAL CURRENCIES

- Crypto coins and crypto currencies have suddenly gained large audiences across the globe. The most prominent amongst them is Bitcoins.

- Bitcoins have seen uneven ride lately with Mt. Gox, Bitcoins exchange, filing for bankruptcy. There are increasing attacks on Bitcoins exchanges and users.

- Thus there is a need to appropriately consider the security legal and other risks in this regard. Different regulators in different parts of the world have already come down heavily on Bitcoins stating that people need to be very careful when they use Bitcoins.

- As Bitcoins crimes are increasing, there is a need for looking at appropriate legal frameworks which can effectively regulate certain activities of Bitcoins and other crypto currencies.
WEARABLE TECHNOLOGIES

© of images belongs to the respective copyright holders
WEARABLE TECHNOLOGIES

- As wearable technologies are going in the mainstream, with the advent of Google glass and other technologies, there are large numbers of legal, policy and regulatory issues that need to be specifically looked at in the context of wearable technologies.
ONLINE CONSUMER PROTECTION

© of images belongs to the respective copyright holders
CONCLUSION

➢ All in all, Cyberlaw and Cybercrime today represent important fascinating aspects of our lives. Cyberlaw and cybercrime jurisprudence is not just limited to lawyers; it is of relevance to every user of the electronic and digital ecosystem as also mobile ecosystem.

➢ Ignorance of law is no excuse in the eyes of law
CONCLUSION

- Only in compliance, compliance and compliance with the Indian Cyberlaw lies the way for Nirvana for any entity dealing with the digital and mobile ecosystem.
A PRESENTATION
BY
PAVAN DUGGAL
ADVOCATE, SUPREME COURT OF INDIA
PRESIDENT, CYBERLAWS.NET
PRESIDENT, CYBERLAW ASIA
HEAD, PAVAN DUGGAL ASSOCIATES
pavan@pavanduggal.com
pavan@pavanduggal.net