Laws relating to Cybercrimes: Advances and bottlenecks

Presentation by

Anand Desai

Introduction

Computers have changed our lives –

- for communication and information sharing, breaking down customs and similar tax barriers, providing the ability to be anonymous, or mask one's identity while communicating, and making available practically unlimited information easily
- For transactions such as banking, travel, ticket booking, gaming
- For e-commerce transactions including retail, which are quickly replacing physical sales outlet models
- For uploading content which may be copyrighted, etc.

Introduction (ctd)

This has also resulted in –

- Personal conversations and letters being replaced to a large extent by emails, sms, whatsapp, social media etc., which are carried instantly and to as wide an audience as desired, but through third party servers, and can be intercepted, changed, and even hijacked through the use of technology
- Computers, smartphones etc., being linked through the internet making it possible for others to access information on your computer device remotely, including by sending you a virus
- Impersonation becoming very easy

Cyber crimes

Cyber crime - any criminal activity in which a computer or computer network is the source, tool, target or place of crime.

Almost all crime involves communication.

Most communication is now through a computer device, including smartphones.

Hence, there is a “cyber” element in most crimes.

The traditional methods and the pace of detecting and solving crimes have changed!

Some current mega cyber crimes

- Earlier this week, HBO was hacked, and the script for the fourth episode in the latest Game of Thrones season leaked. Episodes from other unreleased TV series also leaked, with hackers having stolen as much as 1.5 terabytes of data (estimated to hold about 60 days of videos). Currently each episode of Game of Thrones costs on average $6 million.

- The hackers may have also stolen potentially sensitive information, including employee data, and even access to internal corporate email.

- The hackers published a text document online that proves the have accessed information of a senior HBO executive, including sensitive data like online accounts, online banking, and personal health services

Current mega cyber crimes

- Star India has confirmed the leak of an unreleased episode of the popular HBO show Game of Thrones, after it appeared on the Internet earlier today, 3 days before its official release date.

- The leaked episode that is circulating online bears a Star India watermark throughout the episode along with a "For internal viewing only" warning. It seems this episode was not part of the hack faced by TV network HBO earlier this week.

Current mega cyber crimes

- In June 2017 a global cyber attack, which is being linked to the WannaCry ransomware, affected several companies and countries
- Operations at a Jawaharlal Nehru Port Trust terminal in Mumbai were forced to shut after being impacted in the cyber attack
- In Australia, a Cadbury chocolate factory ground to a halt after computer systems went down
- Security experts said they did not believe that the ransomware had a "kill switch" making it harder to stop than WannaCry

Current mega cyber crimes

- Ransom is demanded in bitcoins - a type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank

- When the master or masters of the WannaCry cryptoransomware worm emptied the bitcoin wallets, they apparently did so to make future movement of the funds more anonymous by exchange for XMR, the "untraceable" private digital currency backed by Monero.

- Monero is a private digital currency focused on anonymity. While it is based on blockchain like other cryptocurrencies and uses distributed consensus for all transactions to prevent wallet hacking, it uses "ring signatures‟, an anonymous cryptographic signature scheme, to sign transactions. This makes it impossible to tell which parties were involved in a transaction

Piracy as a cyber crime

- The film “Dangal” released in theatres around the world on 23 December 2016

- On 24 December it was being shared on facebook

- We sent a notice to facebook, and they pulled it down from the URL (Uniform Resource Locator - the address of a World Wide Web page)

- The police cybercell registered a complaint

- The facebook user who uploaded the video was a Pakistani national living in Dubai. Apparently, he leaked the entire Dangal film online and managed to accumulate more than 8,33,000 views and over 50 shares before it was deleted

Impersonation as a cyber crime

- Aamir Khan was shocked to find an interview attributed to him on several Pakistani websites in relation to his film PK. He had never given such an interview. It was clearly a fabrication by someone trying to impersonate him, done with the intent of drawing visitors to their website, and is defamatory to Aamir

- He filed a complaint with the cybercell, who found one person in Hyderabad who had also published this fake interview.

Some forms of cyber crimes

- Hacking: Hacking is perhaps one of the most pervasive cyber crimes. Hacking simply means unauthorized access of a computer or computer network

- Spamming: Sending unsolicited bulk emails over internet causing overloading and disrupting service

- Phishing: A fraudulent process of acquiring sensitive information such as username, passwords and credit card details in an electronic communication

- Identity Theft and Impersonation: pretending to be who one is not, attributing authorship of material to oneself

- Cyber stalking: harassment on the internet

Some forms of cyber crimes (ctd)

- Corporate Espionage: Theft of business secrets through illegal means

- Spoofing: An act of disguising one computer to electronically look like another computer, in order to gain access to a system that would normally be restricted

- Software piracy: Use of the internet for illegally copying or distribution of counterfeit or other unauthorized software. This form of piracy occurs when the net is used to advertise, offer, acquire or distribute pirated software

- Copyright piracy: Use of the internet for illegally copying or distribution of pirated content

Some forms of cyber crimes (ctd)

- Morphing of images, and sharing them, usually with mal-intent
- Cyber Pornography
- Privacy Violations by disseminating information that is subject to the right of privacy or right to publicity
- Online defamation
- Cyber Terrorism

Some significant threat vectors

Operation Transparent Tribe: The threat group behind these attacks sent spear-phishing mails with current news which are of interest of the target. The links in the mail redirected the victim to sites which dropped a RAT (Remote Access Trojan) in the victim's system named as MSIL/Crimson. This RAT is quite an advanced cyber-espionage tool, capable of stealing various types of data from the local computer and sending it to a different server.

SmeshApp- A smart targeted cyber attack: A mobile application named 'SmeshApp' was used to spy on soldiers of Indian Army. The soldiers were lured through facebook to install this app in their mobiles and once installed all their stored information, phone calls, text messages and even the movements of soldier by their location used to be sent to a server located in Germany and was hosted by a man in Karachi, Pakistan.

Some significant threat vectors

Operation C Major- The actors behind the attack used emails which were sent to Indian military officials and their passport scans, photo IDs, tax information etc. of more than 160 military officers were stolen. The emails contained a PDF file, which after getting downloaded used to install malicious windows executable ‘Trojan’ in the target system, which acting like a key logger sent the data to a Command and Control server, based out of Pakistan.

Issues with Enforcement

- Difficulty in Detection of Crimes – role of victim / complainant
- Masking of Identity – Anonymity
- Volumes of data on the internet
- Awareness of Rights, experience in this area of police, lawyers and judges
- Admissibility of Digital Evidence
- Data protection – once the damage is done how can it be reversed
- Jurisdiction – Territorial, quantum involved, different levels of legal protection in different countries, extra-territorial Jurisdiction

Issues with Enforcement (ctd)

- Nature of emails and social media posts – jurisdiction issues
- Bank frauds – external and internal examples
- Defamation – what was the intent behind the communication
- Masking of Identity – Anonymity
- Tax evasion
- Liability of those who give access to the internet
- Misuse of “secure communication devices”

The Path Ahead

- Introducing technology training so that awareness about the different ways technology can be used is disseminated.
- Educating people about the pitfalls and the negative impact the internet can have.
- Contractual protection.
- Insurance?
- Training police, prosecutors and judicial officers is a must. Cybercells have been a big step forward. Cyberlabs and NASSCOM support has helped in India with initiatives like cyber-safety week.
- Investigations and legal enforcement need to be more sophisticated, and stricter.

Main Laws

- Information Technology Act, 2000 (IT Act).
- Indian Penal Code, 1860 (IPC).
- Rules framed under IT Act.

Enactment of the IT Act

- History of IT Act 2000 - UNCITRAL Model law on E-Commerce
- The Information Technology Act was enacted in the year 2000 with a view to -
  - ➢ Regulate electronic based transactions
  - ➢ Provide legal recognition for e-commerce and e-transactions
  - ➢ facilitate e-governance
  - ➢ to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide
- The IT Act was amended in 2008

Key Provisions under the IT Act

- "Cyber Security" as defined under the IT Act reads as follows:

  "protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction."

- Section 65 to 74 of the IT Act, specifically deal with certain offences, which can be called cyber crimes.

Offences

	Indian Penal Code	IT Act
Threatening emails/stalking	Section 503/354D	--
Defamatory Messages/offensive communication	Section 499	Section 66A is being struck down as unconstitutional.
Bogus Websites/Cyber Fraud	Section 420	Section 66
Email Spoofing	Section 463	Section 66D
Pornography	Section 292	Section 67
Data Theft and Hacking	Section 378, 405 and 420	Section 43 (a) and 43(b)
Cheating by Personation/Identity Theft	Section 419	Section 66C and 66D

Offences (Contd.)

IT Act	
Tampering with any computer source code etc.	Section 65
If your account is hacked	Section 66
Violation of Privacy	Section 66E
Cyber Terrorism	Section 66F
Victim of Identity Theft	Section 66C
Impersonation	Section 66D
Obscenity/Pornography	Section 67
Information must be preserved by Intermediary	Section 67C

Offences (Contd.)

IT Act	
Disclosure of Information in breach of contract	Section 72-A
Publishing electronic signature certificate for fraudulent purpose	Section 74
Offence by Companies	Section 85

Nodal Agencies

- Indian Computer Emergency Response Team (CERT-In) which is to function 24 x7x365 and will serve as national agency for incident purpose for the following functions:

  - collection, analysis and decimation of cyber incidents;
  - forecast and alerts of cyber security incidents;
  - emergency measures for handling cyber security incidents; and
  - issue guidelines, advisories vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

- National Nodal Agency for protection of critical information infrastructure has been identified as "National Critical Information Infrastructure Protection Centre" JNU Campus, New Delhi.

Other provisions

- Indian Government empowered to intercept wireless messages in the interest of national security.

- Persons not below the rank of an Inspector may investigate any offence and / or enter any public place and search and arrest without a warrant.

Rules framed under the IT Act

The Department of Information Technology has notified four sets of rules effective from April 11, 2011.

- IT (Reasonable Security Practices and Procedures and sensitive personal data or information) Rules, 2011 (“**Reasonable Security Practices Rules**”)
  - These lay down the minimum security practices and procedures to be adopted while collecting any sensitive personal information.
- Information Technology (Intermediaries guidelines) Rules, 2011.
  - These provide for the due diligences to be observed by the intermediaries so as to be exempted from liability in certain cases and also provide that an intermediary shall respond within 36 hours of a complaint or grievance being reported.

Rules framed under the IT Act (Contd.)

- The Information Technology (Electronic Service Delivery) Rules, 2011 and Information Technology (Guidelines for Cyber Cafe) Rules, 2011
  - ➢ providing for the electronic delivery of public services by the Government and mandatory due diligences to be observed by cyber cafe owners.

- The Government declared UIDAI's Central Identities Data Repository (CIDR) facilities, Information Assets, Logistics Infrastructure and Dependencies installed at UIDAI locations to be "*Protected System*" for the purpose of IT Act. It has also identified authorized personal who can have access to UIDAI- CIDR facilities.

Rules framed under the IT Act (Contd.)

- Digital Signature (End Entity Rules), 2015 define various terms used in the process & usage of the digital signatures and the process for authentication of information by means of Digital Signature, Creation and Verification of Digital Signature, Digital Signature Standards, etc.

- Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013 for sectors which are critical to the nation and whose incapacitation or destruction will have a debilitating impact on national security, economy, public health or safety. The National Critical Information Infrastructure Protection Centre is the nodal agency in respect of 'Critical Information Infrastructure Protection.

Advisory on functioning of Matrimonial Websites

- Matrimonial websites are to function as "intermediaries" and are brought under the purview of IT Act, and must have:
  - ➢ user agreement (Terms and Conditions) accepted by each user at the time of registration
  - ➢ privacy policy and user verification by registering his or her mobile number
  - ➢ Submission of Identity documents
  - ➢ Submission of declaration that the website is to be used only for matrimonial purpose and not a dating website or for posting obscene material
  - ➢ Display details of grievance officer and complaint redressal mechanism

THANK YOU

Comments and feedback: anand.desai@dsklegal.com

Mumbai Office:
1203, One Indiabulls Centre, Tower 2,
Floor 12-B, 841, Senapati Bapat Marg,
Elphinstone Road,
Mumbai 400013
Tel +91 22 6658 8000
Fax +91 22 6658 8001

Delhi Office:
4, Aradhana Enclave,
R.K Puram, Sector 13,
Opposite Hotel Hyatt,
New Delhi 110 066
Tel +91 11 6661 6666
Fax +91 11 6661 6600

Mumbai Office (Litigation Group):
C-16, Dhanraj Mahal,
Chhatrapati Shivaji Marg,
Apollo Bunder,
Mumbai 400001
Tel +91 22 6152 6000
Fax +91 22 6152 6001

Pune Office:
301, Power Point,
Lane No.6, Koregoan Park,
Pune 411 001
Tel + 91 20 6900 0930

For more details: www.dsklegal.com

Disclaimer

The contents of this document are privileged and confidential and not for public circulation. This document is for general information of our clients and others to whom it is specifically provided. The information contained in this document is derived from public sources, which we believe to be reliable but which, without further investigation, cannot be warranted as to their accuracy, completeness or correctness and we are not obligated to update or amend the same. The information contained in this document is not intended to be nor should be regarded as legal advice and no one should act on such information without appropriate professional advice. DSK Legal accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.