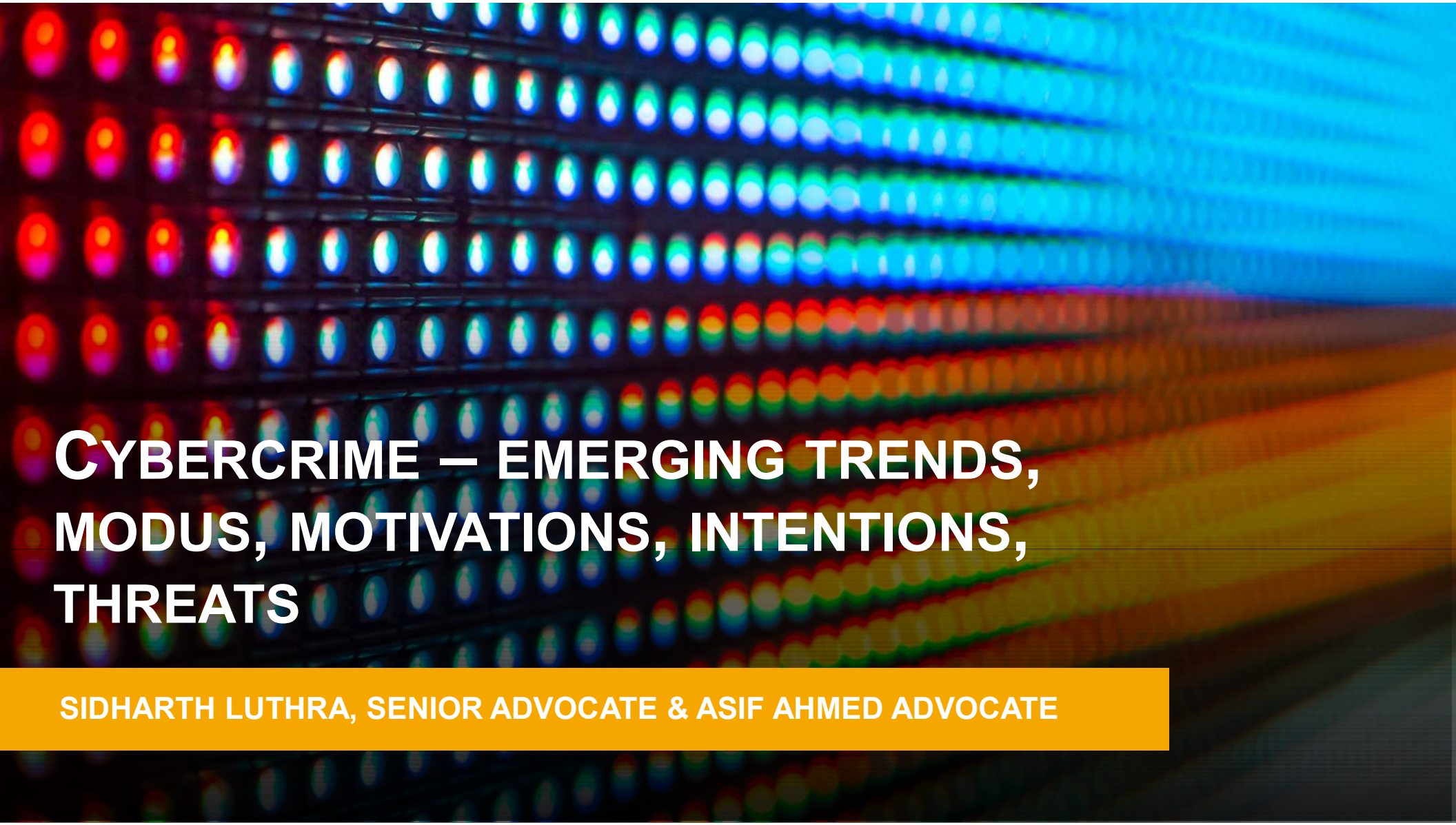


CYBERCRIME – EMERGING TRENDS, MODUS, MOTIVATIONS, INTENTIONS, THREATS

SIDHARTH LUTHRA, SENIOR ADVOCATE & ASIF AHMED ADVOCATE

Trans-national reach of cyber crime cases

CYBER TECHNOLOGY: CLOUD COMPUTING, HASH VALUES AND DARK WEB

RE-DEFINING JURISDICTION

"*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather*."

John Perry Barlow, "A Declaration of the Independence of Cyberspace" (1996)

INTRODUCTION

- In the 20th century, oil was the most valuable commodity. Today, it is data.
- Internet, first developed in the 1960s for the US Defence has within a span of a few decades, become a necessity of life.
- Access to internet - *"Universal basic internet"* is now being touted as the new human right. Universal basic internet aims at providing access to internet to every country, deep within its states, in small villages and to men and women of all strata.
- Internet transcends boundaries, is borderless and stateless.
- While internet has had its benefits, it has given rise to cybercrime which transcends boundaries.

UNITED NATIONS OFFICE ON DRUGS AND CRIME

- Cyber crime offences cluster around the following categories:

i) offences against the confidentiality, integrity and availability of computer data and systems;

ii) computer-related offences;

iii) content-related offences; and

iv) offences related to infringements of copyright and related rights.

- There are cyber-dependent offences, cyber-enabled offences and, as a specific crime-type, online child sexual exploitation and abuse.

i. *Cyber-dependent crime* are creation, dissemination and deployment of malware, ransomware, attacks on critical national infrastructure and taking a website offline by overloading it with data

ii. *Cyber-enabled crime* is that which can occur in the offline world but can also be facilitated by ICT. This typically includes online frauds, purchases of drugs online and online money laundering.

iii. *Child Sexual Exploitation and Abuse* includes abuse on the clear internet, darknet forums and, increasingly, the exploitation of self-created imagery via extortion - known as "sextortion".

INTRODUCTION

- Cyber-crime transcends national and international borders and raises jurisdictional issues that one nation alone cannot address.
- The internet or the cyberspace has changed our sense of place or duration as well as *"the unity of time, place, and action that informed the notion of actus reus in the criminal law"* giving rise to jurisdictional issues in investigation and trial cyber-crimes.
- A physical action of a person behind a computer system in **A** country can have consequences in one or more countries. This raises the issues of investigation of the crime i.e., *investigation of crimes committed with or against computing systems cannot restrict itself to local computing systems especially in light of cloud computing where servers and other delivery systems of a country are located in another country.*

CLOUD COMPUTING - A NEW PARADIGM

- In 2011, the United States Department of Commerce National Institute of Standards and Technology (NIST) described cloud computing as:

  "…….a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"

CLOUD COMPUTING

- Data today maybe used in one country but maybe stored or accessed through servers or resources in another country.
- For e.g., when one uploads his/her data on “cloud”, the data may belong to a person in India, but is hosted in a server in Australia.
- There are issues of privacy, and in relation to cyber crime – issues of reach of investigators as well as the evidentiary value of the material collected.

RE-DEFINING JURISDICTION

- As per James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p. 537, jurisdiction, refers to *"a state's competence under international law to regulate the conduct of natural and juridical persons'.*
- There are five internationally recognised heads of jurisdiction that serve to establish a substantial connection between a State and an individual : the territorial principle, the nationality principle, the protective principle, the universality principle and the passive personality principle.
- As Internet facilitates remote control across national borders, the fundamental assumptions of territorial criminal jurisdiction often fail.

RE-DEFINING JURISDICTION – INAPPLICABILITY OF TERRITORIAL PRINCIPLE

- The argument for universal jurisdiction allows states to act swiftly in prosecuting cybercrimes without being hampered by overly legalistic considerations of jurisdiction, however, the basis of this principle is that the international community agree on the same offences and punishment.
- But in practice it fails. For e.g.,: death sentence may be legal in one country and illegal in another. Even definitions of offences vary.

RE-DEFINING JURISDICTION – INAPPLICABILITY OF TERRITORIAL PRINCIPLE

- For Cyberspace to be territorialized, it only be done by redefining territory in a way that defies the original connection of the notion of territory to the land. The jurisdiction would have to be inclusive and overlapping.

DOMESTIC FRAMEWORK – EVIDENCE GATHERING

TRANS-NATIONAL EVIDENCE GATHERING – WHAT THE FUTURE HOLDS

- Access to electronic evidence in foreign jurisdictions is primarily governed by mutual legal assistance (MLA) arrangements, however, there may be situations where the origin of an attack is unknown, where servers in multiple jurisdictions are involved, or other ‘loss of location’ situations where the principle of territoriality is not applicable.

TRANSNATIONAL EVIDENCE GATHERING – CHALLENGES

- CrPC as well as *Comprehensive Guidelines for investigation abroad and issue of Letters Rogatory (LRs)/ Mutual Legal Assistance (MLA) Request and Service of Summons/Notices/Judicial documents* in respect of Criminal Matters [04.12.2019] provide for overseas evidence gathering
- The formal devices include requests under *mutual legal assistance treaties* ("MLATs"), *letters rogatory* in the absence of a treaty or executive agreement etc.

A. MUTUAL LEGAL ASSISTANCE TREATY

- **Mutual Legal Assistance** is a mechanism whereby countries cooperate with one another in order to provide and obtain formal assistance in prevention, suppression, investigation and prosecution of crime to ensure that the criminals do not escape or sabotage the due process of law for want of evidence available in different countries.
- The Mutual Legal Assistance Treaties (MLATs) in criminal matters are bilateral treaties, entered between the countries for providing international cooperation and assistance.

Figure 1.1: List of countries having MLAT/Bilateral Agreements with India			
Arab Republic of Egypt (2009)	Kingdom of Morocco* (2018)	Republic of Kazakhstan (2000)	Russian Federation (2000)
Bosnia & Herzegovina (2010)	Kingdom of Spain (2007)	Republic of Korea (2005)	State of Israel (2015)
Canada (1998)	Kingdom of Thailand (2004)	Republic of Maldives* (2019)	State of Kuwait (2007)
Commonwealth of Australia (2011)	Kyrgyz Republic (2014)	Republic of Mauritius (2006)	Sultanate of Oman (2015)
Confederation of Switzerland (1989)	Malaysia (2012)	Republic of Singapore (2005)	Ukraine (2003)
Democratic Socialist Republic of Sri Lanka (2010)	Mongolia (2004)	Republic of South Africa (2005)	Union of Myanmar (2010)
French Republic (2005)	People's Republic of Bangladesh (2011)	Republic of Tajikistan (2003)	United Arab Emirates (2000)
Hong Kong Special Administrative Region of the People's Republic of China (2009)	Republic of Azerbaijan (2013)	Republic of Turkey (1993)	United Kingdom of Great Britain and Northern Ireland (1995)
Islamic Republic of Iran (2010)	Republic of Belarus (2006)	Republic of Uzbekistan (2001)	United Mexican States (2009)
Kingdom of Bahrain (2005)	Republic of Bulgaria (2008)	Republic of Vietnam (2008)	United States of America (2005)
Kingdom of Cambodia* (2018)	Republic of Indonesia (2011)		

*The MLAT has been signed but yet to come in force.

TRANS-NATIONAL EVIDENCE GATHERING – STEPS TO BE TAKEN BY INVESTIGATOR

- The first thing an investigator should determine is what formal and informal devices are available to search for and/or seize evidence located in another country.
- Often informal methods are expeditious however limited to countries with friendly relationship/s but may create doubt on evidentiary validity of value of material at trial.

TRANSNATIONAL EVIDENCE GATHERING

- The investigator should therefore identify the country from which evidence is to be sought and determine whether a mutual legal assistance treaty encompassing the evidence exist with that country.
- The procedure for obtaining assistance under an MLAT is "generally faster and more reliable" than the process of using letters rogatory
- A critical issue is determining whether the evidence being sought pertains to conduct that is illegal in the country from whom assistance is requested.
- Some countries only grant assistance if conduct is illegal under their own laws. This can be a significant impediment.

TRANSNATIONAL EVIDENCE GATHERING – SOURCE OF GUIDANCE

LETTERS ROGATORY

- Derived from the Latin term rogatorius.
- Letters Rogatory are the letters of request sent by the Court of one country to the Court of another country for obtaining assistance in investigation or prosecution of a criminal matter.
- **Section 166A and Section 105K of Code of Criminal Procedure, 1973** (CrPC), **Section 57 and Section 61 of Prevention of Money Laundering Act, 2002** (PMLA), **Section 12 of Fugitive Economic Offenders Act, 2018** (FEOA), etc., lay down the procedure of sending 'letter of request' through Competent Court on the request of Investigating Officer.
- The procedure for execution of a request received from a foreign Court or Competent Authority has been enshrined in Section 166B and 105K of CrPC, Section 58 of PMLA, etc.

TRANSNATIONAL EVIDENCE GATHERING – SOURCE OF GUIDANCE

SERVICE OF SUMMONS, NOTICES AND JUDICIAL PROCESSES

- **Section 105** and **Chapter VIIA of CrPC [Reciprocal arrangements for assistance in certain matters and procedure for attachment and forfeiture of property], Section 59 and Section 61 of PMLA**, **Section 10 of FEOA**, etc., provides for service of summons, notices and judicial processes.
- The summons, notices and judicial processes are sent by the Court of competent jurisdiction to IS-II Division, MHA and are further sent by MHA to the foreign country concerned either directly or through Indian Mission/Embassy/Diplomatic Channels for service on the person through the Competent Authorities in the foreign country.

TRANSNATIONAL EVIDENCE GATHERING – SOURCE OF GUIDANCE

MUTUAL LEGAL ASSISTANCE (MLA) REQUEST

- Mutual Legal Assistance Request is a formal request made by the Central Authority of India i.e., Ministry of Home Affairs to the Central Authority of another country on the request of Investigating Officer or Agency under any Bilateral Treaty/Agreement, Multilateral Treaty/Agreement or International Convention.

TRANSNATIONAL EVIDENCE GATHERING – SOURCE OF GUIDANCE

OBTAINING STATEMENT OF A PERSON RESIDENT ABROAD

- A Court in India may issue a commission under Section 285 of CrPC18, subject to the domestic laws of the foreign country.
- Section 161 CrPC provides that the examination of witness may also be done by audio-visual electronic means.
- Also see *State of Maharashtra vs Praful Desai* (2003) 4 SCC 601
- Courts have also allowed investigation through VC (*Roshni Biswas v. Union of India* 2020 SCC Online SC 881)

TRANSNATIONAL EVIDENCE GATHERING – PMLA AND CRYPTO – EG. BITCOIN

- Cryptocurrencies are susceptible to criminal activities like money laundering and terror funding.
- Cryptocurrencies are used to hide source of wealth and for tax evasion.
- Some cryptocurrencies do not keep a database and sources of funds are therefore largely unknown.
- Lack of enforcement oversight and protection and lack of regulatory mechanism makes it a safe haven for criminal activities.
- RBI imposed a ban Vide Notification dated 6-4-2018 (RBI Notification), from dealing in virtual currencies or providing services for facilitating any individual or entity in dealing with virtual currencies. Quashed by Supreme Court in ***Internet & Mobile Assn. of India*** **v. RBI, (2020) 10 SCC 274**.

- CRYPTO digital wallet is where Crypto is kept.
- Crypto & now we have stable coins – linked to currency rate!
- Need to be regulated by linking it to Aadhar/PAN and requirement of keeping record of personal details and transactions as in Section 12 PMLA - requirement to maintain records by Banking companies, financial institutions and intermediaries.
- **S. 2(s)(sa**) PMLA needs to be amended to bring within its scope cryptocurrency exchanges under the definition of *"person carrying on designated business or profession* "and bringing it under **S. 2(w)(wa***) "reporting entity".*

COUNCIL OF EUROPE'S CONVENTION ON CYBERCRIME.

- Efforts underway to improve the efficacy and efficiency of law enforcement cooperation in cybercrime investigations.
- The most outstanding is the **Council of Europe's Convention on Cybercrime**.
    1. Parties to the Convention pledge to adopt whatever measures are needed to ensure the preservation and collection of evidence and the providing of mutual assistance in cybercrime investigations even when no MLAT is in force between the requesting country and the requested nation.
    2. They agree to *"afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."*
    3. The convention ensures that in urgent circumstances, requests for mutual assistance or communications related thereto by expedited means of communications, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, will be honoured by the requested Party.
    4. Non EU countries can join

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a. *access publicly available (open source) stored computer data, regardless of where the data is located geographically; or*

b. *b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.*

CLOUD COMPUTING AND PRIVACY

- The question with cloud computing is who does the data belong to. This creates data privacy issues.
- The **United States' CLOUD Act** provides a framework by which US entities can share data with foreign law enforcement agencies pursuant to an agreement.
- The US Department of Justice's 2019 White Paper on Purpose and Impact of the CLOUD Act states that communications service providers subject to US jurisdiction must disclose data required for valid US legal process, regardless of where the company stores the data. This is to overcome conflict of laws situation and allow sharing of contents of electronic communications with either US or foreign law enforcement agencies, with very limited exceptions.

CLOUD COMPUTING AND PRIVACY

- However, while doing so what is required is a procedure for data privacy and protection of civil liberties. In India, Right to Privacy recognized in the judgment in ***Puttaswamy*** **(2017) 10 SCC 1**.
- The US CLOUD Act requires that while entering into agreement, it will be taken into consideration whether the foreign country is a party to the Budapest Convention on Cybercrime, and if not a party, then if the domestic laws of the foreign country are consistent with the definitions and requirements set forth in that Convention.

CLOUD COMPUTING AND PRIVACY

- The IT Act also provides for data protection under S. 43A of the Act.

  ***"43A. Compensation for failure to protect data.**--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…"*

DARK WEB

- A global network of computers that use a cryptographic protocol to communicate, enabling users to conduct transactions anonymously without revealing their location. Transactions are run through disguised dummy transactions, wherein payments are made through the digital currency Bitcoin.

[Donna Leinwand Leger, *How FBI Brought Down Cyber-Underworld Site Silk Road*, USA TODAY (May 15, 2014, 2:54 PM EDT) ; **Also see**: Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075, 1077]

DARK WEB - LACK OF SOURCE SPECIFICATION : INVESTIGATIVE PARADIGMS

-
- The normative process for detection of a crime committed using the dark web involves tricking the target into downloading malicious code, the commonplace American terminology for which is "network investigative technique" or NIT.
- Using NIT, an investigative agency searches for location information on the target's computer. With the suspect's location (and perhaps identity) revealed, the investigation can focus on that location and proceed in the usual way.

[O.S. Kerr & S.D. Murphy, *Government Hacking to Light the Dark Web : Risks to International Relations and International Law?*, 70 Stan. L. Rev. 58, 59 (since the term NIT has no clear technical meaning, it is assumed that the term refers to software used to bypass security features controlling access to a computer.)]

DARK WEB -PROCEDURAL & EVIDENTIARY IMPEDIMENTS

- S. 166-A, Cr.P.C. : Letter rogatory process can be undertaken, provided the investigative agency undertakes the NIT route. In doing so, the concerned suspect, and any electronic record pertinent to the investigation, may be effectively requisitioned even from a foreign territory.
- Practice suggests a norm of cooperation instead of confrontation vis-à-vis investigation of transnational offences committed via the dark web. [O.S. Kerr & S.D. Murphy, *Government Hacking to Light the Dark Web : Risks to International Relations and International Law?*, 70 Stan. L. Rev. 58, 65]
- While Indian criminal procedure appears ambiguous in respect of search warrants, U.S. federal law stipulates that search warrants may be issued by investigators "*to use remote access to search electronic storage media and to seize or copy electronically stored information.*" [Rule 41(b)(6), Federal Rules of Criminal Procedure]
- This is subject to whether the concerned stored data is (i) publicly available ; or (ii) local law enforcement has obtained consent of the owner of the device. These limitations emanate from Article 32 of the Budapest Convention on Cybercrime [2296 U.N.T.S. 167, ratified by U.S. Senate in September, 2006]

HASH-VALUE & META DATA

- An alpha-numerical identifier (digital fingerprint) that is unique to each electronic file. A hash value does not appear on the face of a document or file but is part of the file's **metadata**. MD5 and SHA are common types of hash values.
- The hash value plays an important role in establishing the authenticity and integrity of data/evidence in the digital world. It is crucial to not only to authenticate the integrity of the data but also plays a crucial role in validating the forensic processes and equipment used for forensic examination.
- Explanation to Section 3:

  "Explanation.–For the purposes of this sub-section, —hash function means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as —hash result such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible–"

EVIDENCE ACT AND EVER-EVOLVING TECHNOLOGY

- Technology is not static. Presently, electronic evidence under the Evidence Act, 1872 is dealt with under S. 65B. Under S. 65B(1), any information that is contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed to be a document, and shall be admissible in any proceedings without further proof of production of the original, as evidence of the contents of the original or of any facts stated therein of which direct evidence would be admissible.
- S. 65B(2) refers to conditions to be satisfied in respect of computer output like computer is regularly used etc.
- Therefore, if the electronic evidence is “original” and fulfils the conditions in sub-section (2) then it is admissible in any proceedings without any further proof or production of the original as evidence of any contents of the original.

EVIDENCE ACT AND EVER-EVOLVING TECHNOLOGY

- Primary known principles may not be sufficient to deal with evolving technology due to issues relating to access of remotely stored data.
- For e.g., - When it comes to technology like blockchain, it is spread over multiple computers all over the world and keeps growing. Therefore, it is impossible to produce it in a way provided under S. 65B. The only option thus is secondary evidence as provided in S. 65B(4).
- However, in a case where the technology is not susceptible to tampering like blockchain technology, it would be essential to provide a certificate for its production.
- The principles of admissibility depend upon the technology being susceptible to tampering or alteration as well as on the principles of original and secondary evidence.

EVIDENCE ACT AND EVER-EVOLVING TECHNOLOGY

- In ***United States v. Lizarraga-Tirado, the Ninth Circuit* 789 F.3d 1107 (9th Cir. 2015)** analysed the use of a Google Maps entry and a computer generated "thumbtack" of a crime scene in an immigration case and held the evidence as admissible on the ground that the technology itself is computer-generated evidence and incorruptible with no human interference. [**Angela Guo, Blockchain Receipts: Patentability and Admissibility in Court, 16, Chi.-Kent J. Intell. Prop. 440 (201)**.]

Liabilities of intermediaries

WHAT ARE INTERMEDIARIES

"Intermediary" is defined under **Section 2(1)(w)** of the I.T. Act, which is as follows: —

> *2(1)(w) —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.*

WHAT ARE INTERMEDIARIES

***Google India (P) Ltd. v. Visaka Industries*, (2020) 4 SCC 162**

"51. ….There are different kinds of intermediaries. They include:

(i) Internet Access and Service Provider (ISP). Examples are given in this category of Airtel, Vodafone, BSNL among others;

(ii) Data Processing and Web Hosting Providers. Examples include GoDaddy and BigRock;

(iii) Internet Search Engines and Portals like Google, Yahoo and Binge;

(iv) Email hosts like Gmail (Google) and Yahoo!Mail;

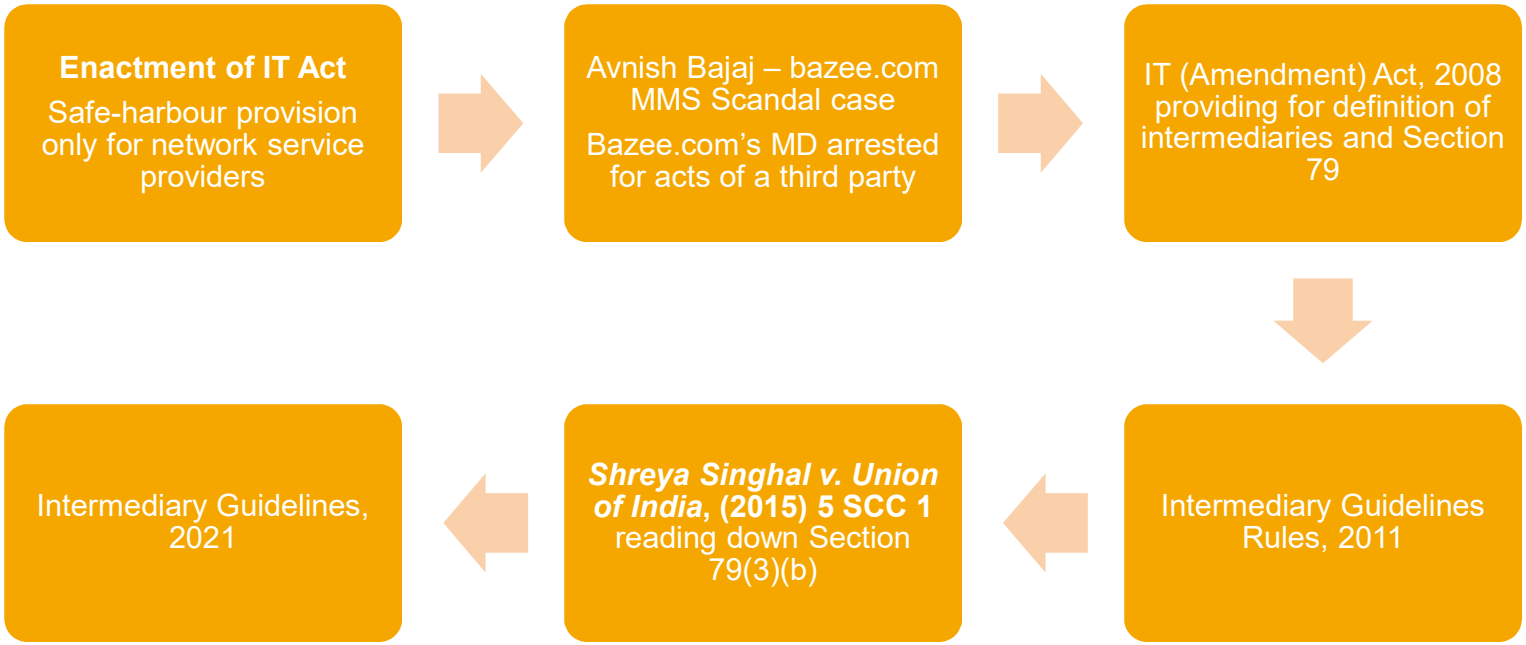
(v) Then there are instant messaging platforms such as WhatsApp, Facebook Messenger, Skype, etc.;

(vi) E-commerce intermediaries where the platforms do not take title to the goods being sold like Amazon India, Flipkart, etc.;

(vii) Internet Payment Systems and Mobile Wallets like Paytm, etc.;

(viii) There are also participative internet platforms."

A BRIEF HISTORY OF INTERMEDIARIES IN INDIA



LIABILITY OF INTERMEDIARIES

- Three broad models of intermediary liability have emerged globally, [Article 19 in 2013 report titled “Internet Intermediaries: Dilemma of Liability”]:

A. The strict liability model: Intermediaries are held unconditionally liable for user-generated content – monitoring of content like China

B. The safe-harbour model: Intermediaries are given conditional immunity from liability arising out of user-generated content i.e., if they comply with certain requirements laid out under law.

(a) The vertical model: Liability is determined according to the type of content at issue.

(b) The horizontal model: Liability is determined according to the kind of function performed by the intermediary.

C. The broad immunity model: Intermediaries are given broad, at times conditional, immunity from liability arising out of user-generated content. Intermediaries are also expressly excluded from any obligation to monitor for unlawful content.

LIABILITY OF INTERMEDIARIES UNDER THE IT ACT

- Section 79 of the original Act only protected network service providers from liability arising from third party content, if they proved absence of knowledge; or application of positive application of due diligence on their part to prevent commission of an offence/ contravention.
- Subsequently, vide the IT (Amendment) Act, 2008, the current Section 79 was enacted providing safe harbour to intermediaries.
- The obligation of an intermediary is provided under **Section 79 of the I.T. Act**, which falls under **Chapter XII** under the title — **Intermediaries Not To Be Liable In Certain Cases**

LIABILITY OF INTERMEDIARIES UNDER THE IT ACT

- One of the triggers for such amendment was the MMS Scandal concerning bazee.com wherein a MMS clip was uploaded on bazee.com which contained sexually explicit content being offered for sale on the website. The then MD of bazee.com was arrested for this act of a third party despite bazee.com only being an intermediary. [*Avnish Bajaj v. State (NCT) of Delhi*, 2004 SCC OnLine Del 1160]
- In the 2005 Report of the Expert Committee, set up by the Ministry of Information and Technology to recommend changes to the IT Act, the rationale for amending the safe-harbour provision i.e., Section 79 was explained as to bring it in line with the EU's Directive on e-commerce (2000/31/EC).

INFORMATION TECHNOLOGY (INTERMEDIARIES GUIDELINES) RULES, 2011

- After the amendment to the IT Act in 2008, which incorporated the 'due-diligence' requirement for intermediaries for claiming safe-harbour, the Government of India issued the **Information Technology (Intermediaries Guidelines) Rules, 2011**.
- The Intermediaries Guidelines, *inter alia*, required adherence to certain condition including (a) Publishing rules/regulations; privacy policies; user agreements; (b) Terms and conditions to specify prohibited content- grossly harmful, harms minors, infringes intellectual property rights, contains virus etc. (c) A strict notice and takedown process; (d) Assistance to government agencies for law enforcement; (e) A duty to report cyber security incidents to the government; and (f) Appointment and notification of a grievance officer.

Shreya Singhal and narrowing the scope of ‘actual knowledge’

- *In* ***Shreya Singhal v. Union of India*****, (2015) 5 SCC 1,** Section 79 was under challenge. While upholding the validity of Section 79, the Supreme Court held that the the provision would be valid subject to it being read down as under:

> *“122. Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material. This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook, etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not. We have been informed that in other countries worldwide this view has gained acceptance, Argentina being in the forefront. Also, the Court order and/or the notification by the appropriate Government or its agency must strictly conform to the subject-matters laid down in Article 19(2). Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79. With these two caveats, we refrain from striking down Section 79(3)(b).”*

Shreya Singhal and narrowing the scope of ‘actual knowledge’

Following ***Shreya Singhal***, recently the High Court of Delhi [Order dated 17/08/2022] in **Flipkart Internet Pvt. Ltd. v. State of NCT of Delhi** held that a mere complaint to the intermediary for trademark or copyright infringement is not enough. A court order is required to take down the content:

> *”27…If such a complaint, per se, was sufficient to take down the infringing material, etc., the havoc that can be caused to e-commerce is beyond imagination.*
>
> *28. The contention of the learned senior counsel for the petitioner is upheld that the obligation to take down the offending material/sites, etc., from their platform would arise only on service of a court order upon them, which admittedly, is absent in the present case. This would be in keeping with the views taken by the courts consistently since the judgment in Shreya Singhal (supra). “*

It further held that disobedience of such order of the court would not amount to a criminal offence, for which an FIR can be registered.

Shreya Singhal and narrowing the scope of ‘actual knowledge

Similar findings also in

1. **Kunal Bahl and Anr. Vs State of Karnataka** (Criminal Petition No. 4676 of 2020 and 4712 of 2020)
2. **Kent RO Systems Ltd. and Anr. vs. Amit Kotak & Ors.** (2017) 240 DLT 3

DEPARTURE FROM SHREYA SINGHAL AND EXPANSION OF OBLIGATIONS OF INTERMEDIARIES

- In ***Sabu Mathew George v. Union of India*, (2017) 7 SCC 657**, the Supreme Court placed an obligation on intermediaries to **develop a system of auto-block** so that no one can enter/see the said advertisement or message or anything that is prohibited under the Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994.

  "In our considered opinion, they are under obligation to see that the "doctrine of autoblock" is applied within a reasonable period of time. It is difficult to accept the submission that once it is brought to their notice, they will do the needful. It need not be overemphasised that it has to be an in-house procedure/method to be introduced by the Companies, and we do direct."

THE INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021

- In February 2021, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were enacted primarily aiming at regulating social media intermediaries, such as messaging services and media-related intermediaries such as digital media house.
- The Rules provided **three months** timeline to social media intermediaries to comply with the New IT Rules thereby making all social media platforms to comply with the new Rules.
- Some of the highlights of the rules are:

THE INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021

- **Due diligence** to be followed like

a) publishing rules, regulations, privacy policy and user agreements,

b) inform users not to publish/upload prohibited, illegal or false content,

c) provide information under its control or possession as soon as possible, but not later than seventy-two hours of the receipt of an order to the Government agency which is lawfully authorised for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences; and

d) Report cyber security incidents and share related information with the Indian Computer Emergency Response Team etc.

- **Formation of Grievance redressal mechanism of intermediary**
- It also provides for the **Code of Ethics and Procedure and safeguards in relation to digital media**

THE INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021

- **Additional due diligence to be observed by significant social media intermediary i.e.,**
- appoint a Chief Compliance Officer who shall be responsible for ensuring compliance with the Act,
- appoint a nodal contact person for 24×7 coordination with law enforcement agencies and officers to ensure compliance to their orders or requisitions made in accordance with the provisions of law or rules made thereunder.
- appoint a Resident Grievance Officer, who shall, subject to clause (b), be responsible for the functions referred in **Grievance redressal mechanism of intermediary**.
- publish periodic compliance report every month
- Proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct
- They shall enable to identify the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction.

THE INTERMEDIARY GUIDELINES, 2021 – CHALLENGE

- The rules ex-facie departure from Shreya Singhal in as much as they move beyond “actual knowledge” and safe-harbour principle and move towards a strict liability approach to intermediaries;
- This amongst other things has made them subject to challenge before various HCs. Vide order dated 09.05.2022, the Supreme Court has restrained HCs to hear the challenge to the rules and thus the rules are for consideration before the SC

THE INTERMEDIARY GUIDELINES, 2021 – CHALLENGE

Some of the grounds of challenge are:

- The Intermediary Rules, 2021 seek to undermine end to end encryption which is a subset of fundamental right to privacy as enshrined in *Justice K.S. Puttaswamy vs. Union of India* (2017).
- That there was a lack of stakeholder consultation in contravention of the Government of India's Pre-Legislative Consultation Policy.
- The rules are in contravention to *Shreya Singhal V. Union of India* (2015).
- The Intermediary Rules, 2021 are a delegated legislation and are ultra vires as they are inconsistent with the Information technology Act, 2000 i.e. the parent legislation.
- The Intermediary Rules, 2021 also place an adjudicatory role on intermediaries.

INTERMEDIARIES – ACTIVE AND PASSIVE ROLE

- In ***Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd*., 2020 SCC OnLine Del 454** held that there is no distinction between a passive or active intermediary under S. 79 of the IT Act. This was in light of the finding of the Single Judge that Amazon was a massive facilitator and played an active role in the sales process.

THANK YOU