Cross Border Data-Sharing and India

A Study in Processes, Content and Capacity

By **Amber Sinha, Elonnai Hickok, Udbhav Tiwari and Arindrajit Basu**
Research Assistance **Sarath Matthew and Navya Alam**
Visualisation **Saumyaa Naidu**

The Centre for Internet and Society, India

Cross Border Data Sharing and India - A Study in Processes, Content and Capacity

Centre for Internet and Society, India

Executive Summary

A majority of criminal investigations in the modern era necessitate law enforcement access to electronic evidence stored extra-territorially. The conventional methods of compelling the presentation of evidence available for investigative agencies often fail when the evidence is not present within the territorial boundaries of the state. The crux of the issue lies in the age old international law tenet of territorial sovereignty.Investigating crimes is a sovereign act and it cannot be exercised in the territory of another country without that country's consent. Certain countries have explicit statutory provisions which disallow companies incorporated in their territory from disclosing data to foreign jurisdictions. United States of America, which houses most of the leading technological firms like Google, Apple, Microsoft, Facebook, and Whatsapp, has this requirement.

This necessitates a consent based international model for cross border data sharing as a completely ad-hoc system of requests for each investigation would be ineffective. Towards this, Mutual Legal Assistance Treaties (MLATs) are the most widely used method for cross border data sharing, with letters rogatory, emergency requests and informal requests being other methods available to most investigators.

While recent gambits towards ring-fencing the data within Indian shores might alter the contours of the debate, a sustainable long-term strategy requires a coherent negotiation strategy that enables co-operation with a range of international partners. This negotiation strategy needs to be underscored by domestic safeguards that ensure human rights guarantees in compliance with international standards, clear capacity and clear articulation of how India's strategy lines up with the existing tenets of International law.

This report studies the workings of the Mutual Legal Assistance Treaty (MLAT) between the USA and India and identifies hurdles in its existing form, culls out suggestions for improvement and explores how recent legislative developments, such as the CLOUD Act might alter the landscape. The path forward lies in undertaking process based reforms within India with an eye on leveraging these developments to articulate a strategically beneficial when negotiating with external partners.As the nature of policing changes to a model that increasingly relies on electronic evidence, India needs to ensure that it's technical strides made in accessing this evidence is not held back by the lack of an enabling policy environment. While the data localisation provisions introduced in the draft Personal Data Protection Bill may alter the landscape once it becomes law, this paper retains

its relevance in terms of guiding the processes, content and capacity to adequately manoeuvre the present conflict of laws situation and accessing data not belonging to Indians that may be needed for criminal investigations.As a disclaimer,the report and graphics contained within it have been drafted using publicly available information and may not reflect real world practices.

Introduction

The proliferation of Information Communication Technologies (ICTs) in the twenty-first century and the burgeoning 'cyberspace' has come to form an epoch-defining phenomenon to be addressed by politicians, businesses and law enforcement officials all over the globe. As day-to-day transactions in business, trade, politics and our personal lives become increasingly dependent on digital technology as a medium of transfer, greater amounts of personal information become available on cyber networks. Increased reliance on the internet has thus enabled businesses and governments to alter the manner in which data is collected, shared and utilized Cross border data transfer mechanisms transmit data from one point to another through multi-nodal transmit mechanisms, all of which are located in different jurisdictions. Due to this scattering, the laws of one jurisdiction cannot set the standards for data protection for transfers across the globe. While the internet dilutes the scope for the exercise of sovereign jurisdiction, an entirely borderless internet potentially leaves a vacuum with respect to the enforcement of mechanisms that protect the security of data transferred or stored online. Similarly, excessive data localization fetters the flow of data from one country to another and the significant economic value derived from it.

The construct has altered the nature of some kinds of crime and consequently, the means and methods of criminal investigation and law enforcement in the modern day. To solve crimes in today's age, investigative agencies need to have access to data which is often not in the possession of the accused but may be located in a different jurisdiction altogether.. . The system of trials, since its conception, allow for coercing third parties to obtain evidence material to the trial.[1] If the data were stored in servers located in India, the police in India could have issued an order under §91 of the Code of Criminal Procedure, 1973 ('CrPC') compelling the company to disclose stored information or order an interception,monitoring or decryption order under Section 69 of the IT Act for access to real time data

[1] L. Song Richardson, *Convicting the Innocent in Transnational Criminal Cases : A Comparative Institutional Analysis Approach to the problem* (26 (1) Berkeley Journal of International Law 62, 2008), p.74.

With the advent of economic liberalization on a global scale, however, companies no longer operate within the geographic boundaries of the countries they are incorporated in. To improve cost efficiency and expand the scope and reach of their operations, companies offer services in multiple countries and split their operations across multiple countries. This means first that its users are not confined to the country it is incorporated in, and second,that its servers often exist in a multitude of countries and the data of the user can be stored in any of these countries. The advancement of technology has also resulted in a range of types of data that a communications provider will handle and store. This includes metadata and content data and data in transit and data at rest.

The conventional methods of compelling the presentation of evidence available for investigative agencies often fail when the evidence is not present within the territorial boundaries of the state. The crux of the issue lies in the age old international law tenet of territorial sovereignty.Investigating crimes is a sovereign act and it cannot be exercised in the territory of another country without that country's consent. Certain countries have explicit statutory provisions which disallow companies incorporated in their territory from disclosing data to foreign jurisdictions. United States of America, which houses most of the leading technological firms like Google, Apple, Microsoft, Facebook, and Whatsapp, has this requirement[2].

This necessitates a consent based international model for cross border data sharing as a completely ad-hoc system of requests for each investigation would be ineffective. Towards this, Mutual Legal Assistance Treaties (MLATs) are the most widely used method for cross border data sharing, with letters rogatory, emergency requests and informal requests being other methods available to most investigators.

The subsequent essay analyses the MLAT process from India to the US and back, challenges that this system faces, and proposes possible reforms for India against the backdrop of emerging solutions at the global level. The essay first explores the various theories of jurisdiction in international law which may be relevant for the cross-border data sharing framework. Since a majority of the companies that house data are incorporated in the US, a larger importance is given to the India US MLAT in this policy brief, while at the same time exploring the dynamics of the issue in Europe.

[2] *See* Stored Communications Act, 1986.

This essay does not examine the potential impacts of proposed data localisation measures on the cross-border data sharing landscape as the holistic analysis of this issue deserves treatment in its own right. Instead, the scope of this paper is limited to examining the content, capacity and processes of existing mechanisms.

Overview of Cross Border Data Sharing

Extra-territorial jurisdiction in International Law

Debates on the normative constructs of jurisdiction stretch back perhaps to the origins of international law itself.[3] It has been clearly established that the State is the exclusive agent in the exercise of jurisdiction.[4] Further the Permanent Court of International Justice (PCIJ) clearly stipulated in the *Island of Palmas* arbitration award that a State has exclusive competence with regard to the enforcement of legal, executive or administrative jurisdiction in its own territory. [5]The issue becomes a question of international law therefore when the State attempts to regulate matters that are beyond its territory. In the equally renowned *Barcelona Traction* judgment, the International Court of Justice (ICJ) recognized that the principles of state-sovereignty and the non-interference principle prevented the exercise of jurisdiction outside a state's own territory.[6] There are two approaches to the exercise of jurisdiction. The first approach is enshrined in the landmark *Lotus* Judgement of the PCIJ where it was held that a state may exercise jurisdiction unless it was specifically limited by a prohibitive rule to the contrary.[7] The more commonly followed approach found in state practice however is that states are prohibited from exercising jurisdiction unless there is a positive rule that permits them to do so.[8] This is in line with the presumption against extra-territoriality echoed in *Barcelona*

---

[3] Michael Akehurst, "Jurisdiction in International Law" 46 *British Yearbook of International Law* (1972-73) 145

[4] Menno Kamminga, 'Extraterritoriality', in Wolfrum, R. (ed.), *Max Planck Encyclopaedia of Public International Law*, (Oxford University Press, Oxford, 2010);10

[5] Island of Palmas Case (or Miangas), *United States v Netherlands,* Award, (1928) II RIAA 829, ICGJ 392 (PCA 1928), 4th April 1928, at 838;

[6] *Barcelona Traction, Light and Power Company, Limited*, Judgment, I.C.J. Reports 1970, p. 3.

[7] *S.S. Lotus (Fr. v Turk.) 1927 P.C.I.J.* (ser A) No 10 (Sept 7)

[8] *Arrest Warrant* (Joint separate opinion of Judges Higgins, Kooijmans and Buergenthal), paras 49-50 and Dissenting opinion of Judge ad hoc Van den Wyngaert, para 51; Crawford, James, *Brownlie's Principles of Public International Law*, OUP: Oxford, 2012, p. 486.

Traction and is plays a pivotal role in safeguarding, at least normatively, the sovereign equality of all states.

As per the permissive approach, a state should have a genuine and substantial connection with the situation over which it is seeking to enforce its jurisdiction.[9] Further, the State exercising jurisdiction must have the strongest connection-by way of a regulatory interest or nexus to a situation over which multiple states could claim jurisdiction. [10] Permissive principles of jurisdiction relate therefore to the links between a situation and the concerned state's authority to enforce its jurisdiction in the circumstances. The four core permissive principles are territoriality-where an act is initiated (objective territoriality) or consummated (subjective territoriality), an individual's nationality (jurisdiction based on nationality); the protection of a state's vital interests (protective jurisdiction); the impacts of an extra-territorial act occurring in the state seeking to exercise jurisdiction (effects doctrine) and crimes that violate peremptory norms known as *jus cogens* (universal jurisdiction.) In theory, universal jurisdiction is the only category that can admit extra-territorial jurisdiction without any connection between a situation and its regulation.

The principles of International Law do not seem to indicate a hierarchy between these permissive principles and instead leaves it upto contextually determined agreements to resolve a conflict of laws situation.[11] There is still a fair deal of theoretical confusion regarding extra-territorial jurisdiction, which has been famously described by Prosser as "theorizing about mysterious matters in a strange and incomprehensible jargon."[12] The relative weight given to each permissive principle is a direct function of the underlying motives and values of the key stakeholders and could end up in an ambiguous circle. The same, can however, be said of any International Law standard-simply because as a construct, it is driven by consensus and must incorporate the views of a variety of stakeholders. It's raison d'etre lies, not in creating a panacea that will resolve all conflicts but as a framing device that can serve as an edifice for drawing up agreements that work contextually. Ryngaert advocates for a 'rule of reason' that enables courts and regulators to balance the various interests in each case.[13] Using the principles as a frame of

[9] Arthur Lenhoff, International Law and Rules on International Jurisdiction , 50 Cornell L. Rev. 5 (1964) 18

[10]Cedric Ryngaert,, *Jurisdiction in International Law* (2nd ed , Oxford, Oxford University Press,2015) 10

[11] Christopher Kuner, Extra-territoriality and International Data Transfers in EU Data Protection Law , International Data Privacy Law, Vol 5 Issue 4 Nov 2015, 235-245, 241

[12]William L.Prosser, " Interstate Publication" 51 Michigan Law Review 959,971, 1952-53

[13] Cedric Ryngaert, *Jurisdiction in International Law* (2nd ed , Oxford, Oxford University Press,2015) 10

reference works well in cyberspace as we continue to grapple with the essence of the phenomena itself. Relying on these principles enable global stakeholders to use a common baseline understanding of jurisdiction issues to articulate their positions, which makes the International Law on this aspect both important and worth comprehending-to strengthen India's diplomatic position in cyberspace.

Cyberspace has become the leading example of a phenomenon that is difficult to link directly with physical territory as all transactions over the internet will include some element of extra-territoriality. It has been recognized as the vanguard of the era of transnationalism and globalization and the morphing of barriers created by the Westphalian conception of the nation state. Yet, while jurisdiction may not be imposed over cyberspace itself, individuals using the internet must always remain under the jurisdiction of one state or the other. Therefore, the location of the entry point of data into cyberspace, which in most cases are internet servers, should act as the point of origin of a state's jurisdiction. The consequent conflict revolving around this conception has fuelled many legal and diplomatic tussles in the recent past.

Indeed, one of the greatest regulatory challenges of the internet in the modern day era is to define the extent to which the state can have access to data stored in the cloud. In his seminal work, *Against Data Exceptionalism*, Andrew K. Woods argues that despite the wizardry of the notion of the cloud itself, it is essentially a network of storage devices that are bolted to a specific territory. [14] Data can certainly be thought of as a physical subject-as an intangible asset such as money or doubt, which flows easily across borders. Therefore, it is indeed fair to assert jurisdiction over data by applying the traditional principles of international law rather than resorting to the extremes of excessive localization or an exceptional treatment of data that automatically modifies the regulatory authority of the state and consequently leads to a state of cyber anarchy.

The incentive structure for states to cooperate in the field of cross-border data transfers lies in developing concrete agreements between states leading to the fermentation of universal standards which clearly delineate the types of data and the nature of access that foreign law enforcement authorities have to various types of data. While there is potential for conflict between the various kinds of jurisdiction prescribed by international law, regulatory certainty through municipal law-both substantive and procedural, could weed out this tension, as long as the provisions giving various stakeholders claims to access data are founded on an established conception of jurisdiction.

[14] Andrew K. Woods, " Against Data Exceptionalism", 68 Stanford Law Review 729 (2016),4.

The e-evidence directive proposed by the European Commission on April 17 2018 that makes it easier for law enforcement and judicial authorities of member states to obtain electronic evidence is an example of a workable regional instrument that grapples with these issues. The learnings from the e-directive cannot be juxtaposed into other contexts as the extent of integration within the European Union is unparalleled. However,broad principles that can be moulded to fit into other contexts can be used as learnings. These include[15] **(1) Crafting a European Production Order:** Allow judicial authority in one state to obtain electronic evidence directly from a service provider or legal representative in another state; **(2) Creation of a European Preservation Order:** This will allow an authority in one state to request a service provider or legal representative to preserve specific data in relation to a subsequent data production request, **(3) Incorporation of strong safeguards:** The rules mandate guarantees for the protection of fundamental rights and provision of legal remedies, **(4)Legal certainty for businesses and service providers** by ensuring a uniform set of rules apply to and they come with sufficient clarity.

The four main Indian statues-the Information Technology Act, Indian Penal Code, Code of Criminal Procedure and the Draft Data Privacy Bill appear to defer to all four permissive principles. (Table 1)In the limited sample of cases surveyed,it appears that the Courts have also endorsed these permissive principles, although they may not have explicitly referred to the enabler in international law. An incongruity lies in the Vodafone judgment, which required the establishment of a legal nexus for the Indian revenue authorities to have jurisdiction,although the nature of this nexus remains unclear. Like in international law, Indian law is yet to clearly pronounce a position that might hierarchise the various permissive principles. While a clear hierarchisation is not possible given the vagaries of international law on the matter nor necessary,a coherent approach that illustrates the application of each principle is imperative, given the large number of permissive principles that might be applied to enforce jurisdiction in a cross-border data access issue.

Table 1: Extra-territorial jurisdiction of key statutes

STATUTE	PROVISION	EXPLANATION
INFORMATION TECHNOLOGY	Section 1(2) stipulates that the Information Technology	The IT Act acknowledges all permissive principles of

[15]https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

ACT, 2000	Act: "shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention hereunder committed outside India by any person." Section 75(1) stipulates: "The provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality" Section 75(2) further stipulates: "Further this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India"	jurisdiction. Section 1(2) casts a wide net to ensure that it's application is not prohibitive. Section 75(1) recognizes subjective territoriality, objective territoriality and the effects doctrine by stating that nationality is no bar. Section 75(2) explicitly incorporates the effect doctrine.
THE PERSONAL DATA PROTECTION BILL,2018	Section 2 (1) This Act applies to the following— (a) processing of	The jurisdiction of the Bill under Section 2 includes both territorial and extra-territorial provisions, like the GDPR. It's

	personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India; and (b) processing of personal data by the State, any Indian company, any Indian citizen or any person or body of persons incorporated or created under Indian law.	jurisdiction extends to (1)processing within India and (2) any processing by the State, Indian companies or Indian citizens. In terms of permissive principles with regard to extra-territorial application,it applies to any entities providing goods and services in India, and also to any activity involving the profiling of persons in India. In doing so, it utilises all permissive principles of jurisdiction in international law.
INDIAN PENAL CODE, 1860	Section 4 of the IPC stipulates: "Extension of Code to extra-territorial offences. —The provisions of this Code apply also to any offence committed by— [(1) any citizen of India in any place without and beyond India; (2) any person on any ship or aircraft registered in India wherever it may be;] [(3) any person in any place without and beyond India committing offence targeting a computer resource located in India	As a result of section 4, the IPC extends beyond the territorial limits of India. Procedural steps including inquiry and Investigation and arrest are conducted in pursuance of Sections 4 and 188 of the CrPC This section applies the Nationality principle as iIt deals with conduct of Indian citizens in foreign territory. Further, it regulates the action of any person irrespective of his/her nationality, if such person happens to be on a ship or aircraft registered in India

CRIMINAL PROCEDURE CODE, 1973	Sections 188 When an offence is committed outside India- (a) by a citizen of India, whether on the high seas or elsewhere; or (b) by a person, not being such citizen, on any ship or aircraft registered in India, he may be dealt with in respect of such offence as if it had been committed at any place within India at which he may be found: Provided that, notwithstanding anything in any of the preceding sections of this Chapter, no such offence shall be inquired into or tried in India except with the previous sanction of the Central Government. the expression "computer resource" shall have the meaning assigned to it in clause (k) of sub-section (1) of section 2 of the Information Technology Act, 2000.] Section 179: "179. Offence triable, where act is done or consequence ensues: When an act is an offence by reason of anything which has been	Section 188 of the CrPC is the procedural counterpart of section 4 of the Indian Penal Code and applies the nationality doctrine. Section 179 embodies the effects doctrine as it envisages a scenario where the act done and the consequence felt are in two jurisdictions.

	done and of a consequence which has ensued, the offence may be inquired into or tried by a court within whose local jurisdiction such thing has been done or such consequence has ensued	

Table 2: Principles of extra-territorial jurisdiction endorsed by the judiciary

NAME OF CASE AND CITATION	KEY FACTS AND ISSUES	RELEVANT PARAGRAPHS
Vodafone International Holdings v Union of India (2012) 6 SCC 613	The issue before the Supreme Court was whether the Indian revenue authorities had requisite jurisdiction to tax an offshore transaction of transfer of shares between two non-resident companies where the transaction enables the acquisition of the controlling interest of an Indian company.	*In the instant case, undisputedly, CGP share was transferred offshore. Both the companies were incorporated not in India but offshore. Both the companies have no income or fiscal assets in India, leave aside the question of transferring, those fiscal assets in India. Tax presence has to be viewed in the context of transaction in question and not with reference to an entirely unrelated transaction. Section 195, in our view, would apply only if payments made from a resident to another non-resident and not*

		between two non-residents situated outside India. In the present case, the transaction was between two non-resident entities through a contract executed outside India. Consideration was also passed outside India. That transaction has no nexus with the underlying assets in India. In order to establish a nexus, the legal nature of the transaction has to be examined and not the indirect transfer of rights and entitlements in India. -Paragraph 189 From this case, it appears that the 'effects doctrine' has been recognised but a supposed legal nexus needs to be established for Indian tax authorities to have jurisdiction.
Republic of Italy v Union of India (2013) 4 SCC 721) ('Italian Marines Case')	Indian fishermen were shot dead by Italian Marines on board the Enrica Lexie in international waters.The marines were brought to Indian territory. The Supreme Court had to decide whether the Indian Parliament and courts had	" *I am of the opinion that the Parliament, undoubtedly, has the power to make and apply the law to persons, who are not citizens of India, committing acts, which constitute offences prescribed by the law of*

	jurisdiction in the matter.	*this country, irrespective of the fact whether such acts are committed within the territory of India or irrespective of the fact that the offender is corporeally present or not within the Indian territory at the time of the commission of the offence. At any rate, it is not open for any Municipal Court including this Court to decline to apply the law on the ground that the law is extra-territorial in operation when the language of the enactment clearly extends the application of the law.*" (Judgment, para 29) Even though the Supreme Court did not do so explicitly,this is a clear recognition of the 'effects doctrine' in international law, which indicates that irrespective of where the crime takes place
AV Mohan Rao &Anr v M. Kishan Rao (2002) 6 SCC	Jurisdiction of Indian penal laws over crimes	Ability of the courts to exercise jurisdiction over

174	committed by Indians in foreign territories	individuals or territories is undisputed. Beyond the territory, the High Court admitted that the enforcement is more complicated but strongly affirmed the nationality principle, which indicates that they would have jurisdiction over.
M/S Haridas Exports v All India Float Glass Manufacturers (2002) 6SCC 600	Case was filed before the MRTP (Monopolies and Trade Restrictive Practices) Commission (now Competition Commission of India against three Indonesian companies manufacturing floating glass and selling at predatory prices in India. Question of MRTP Commission's Jurisdiction was challenged before the Supreme Court of India	*It is possible that persons outside India indulge in such trade practices, not necessarily restricted to the* effect*uation of prices within India, which have the* ***effect*** *of preventing, distorting or restricting competition in India or gives rise to a restrictive trade practice within India then in respect of that restrictive trade practice, MRTP Commission will have jurisdiction.* (Clear recognition of effects doctrine)

Types of Data and Access

The three major kinds of data that are usually generated by digital communications are metadata, transactional data and content data. Metadata includes subscriber information, names, email IDs, telephone numbers and and IP addresses associated with an account, both at the time of creation and subsequent usage. Transactional data includes information generated about communications carried out within an

account, such as origin IP address, destination IP address, timestamps, length (size), etc. Finally, content data includes substantial information about the actual content of communications which includes text, pictures, video, audio or any other kind of data that can be used to convey tangible meaning in an interaction. Many legal frameworks have distinct standards for access by law enforcement to the different types of data, such as the ECPA in the USA.

a) Mutual Legal Assistance Treaties (MLATs)

MLATs are binding treaties entered into between nations for seeking and providing assistance for helping each other with domestic legal processes..[16] MLATs envisage a wide range of assistance including serving of summons, taking witness testimony, execution of decrees etc. However, following the scope of this policy brief, the analysis will be focussed on MLATs' contribution to cross border data sharing. Most MLATs have provisions contained in them for the requested state collecting evidence and handing over the evidence to the requesting state.[17] In the absence of any specific provisions for data sharing, these are the provisions that enable cross border data sharing for investigative agencies.

Requests under most MLATs in existence and all the MLATs entered into by India are transmitted between designated Central Authorities in both the states. The Central authority for MLATs related to criminal matters in India is the Ministry of Home Affairs ('MHA'). The procedure with respect to transmission of MLAT requests are given by the MHA in its Letter No. 25106/17/2017 dt. 11th February, 2009.[18] The same is as follows.

An investigative agency seeking to obtain evidence from outside must first obtain a valid summons, warrant, or other judicial process. §105 of the CrPC allows for extra territorial application of summons, warrants or judicial processes issued in India in a manner envisaged by the Central Government. MLATs represent this manner envisaged under §105. This summons along with a covering letter from the Registrar of the Court has to be submitted to the MHA. If the treaty with the relevant country

[16] *See* The Budapest Convention on Cybercrime (European Treaty Series - No.185, Budapest 23.XI.2001); Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (Official Journal of the European Communities, 2000/C 197/01).

[17] Article 15 of the India-US MLAT, available at http://www.cbi.gov.in/interpol/mlat/UnitedStatesofAmerica.pdf; Article 8 (2) (c) of the India-UK MLAT, available at http://www.cbi.gov.in/interpol/mlat/UnitedKingdom.pdf; Article 10 (2) of the India-Israel MLAT, available at http://www.cbi.gov.in/interpol/mlat/Israel.pdf.

[18] Available at <http://mha.nic.in/sites/upload_files/mha/files/pdf/Guid_service_pro250309.pdf>

allows for direct communication between central authorities, then MHA will send the treaty directly to the central authority of that country. Otherwise, the request goes through the diplomatic mission of India in that country. The remaining process within the requested state depends on the laws and institutional structures present in the requested state. Once the Central authority in the requested state receives the results of the request, the same is communicated to the investigating agency through the same chain that it was initiated.

The covering letter accompanying the summons must have a narration of the facts involved in the case and details of the offence. There should also be sufficient information to identify the evidence sought for. When the request is to countries that do not have English as their official language, a certified translation of the letter must also be provided. Though the MHA guidelines do not explicitly say it, logic dictates that the framer of the request will also have to understand the domestic legal process of the requested state and frame the narration of facts in a manner that satisfies such requirements. For example, an MLAT request to US should show facts in such a way that satisfies the probable cause standard.[19]

b) Letters Rogatory

Letters of Rogatory are judicial requests by a court trying a case, directed to a foreign court to take measures to collect evidence for the requesting court's benefit. Under Indian law, §166A of the CrPC allows investigating agencies to approach any criminal court requesting the court to issue an LR to the foreign court where the evidence is located. Thus, an investigative agency can seek an LR by an Indian court requesting a US Court to order Whatsapp to release data from its servers. Prima facie, this solves the problem of evidence procurement.

To understand any shortcomings that may exist with LRs, one must understand how LRs operate and compare them to the consistency, speed and efficiency of the MLAT system. MHA Letter No.25016/14/2007[20] defines how transmission of LRs take place in India. The process envisaged in the document is as follows. It is mandatory that investigative agencies first apply to the MHA before requesting a court under §166A. Before making an application, the investigating officer is supposed to find out whether there are any official channels of data sharing that exists between India and

[19] Bedavyasa Mohanty & Madhulika Srikumar, *Hitting Refresh Making India-US data sharing work* (ORF Special Report, August 2017), p.21.

[20] Available at <http://mha.nic.in/sites/upload_files/mha/files/pdf/LR-170709.pdf>

the country which houses the evidence. The existence of these channels does not compel them to utilise any one of them, as they are free to choose which one they deem to be most appropriate. These channels can be MLATs or Memorandum of Understandings. The investigator is also tasked with finding out whether the requested country has any specific requirements for disclosing evidence like dual criminality, or a probable cause standard. The International Police Corporation Cell of the CBI is the body tasked with providing assistance to any investigating officer who may need it in this behalf.

In addition to the result of the enquiries made in the preceding paragraph, the investigator has to fill in the facts of the case (along with an English copy of the FIR), justify why the obtainment of such evidence is required for continuation of investigations, and also give the suggested procedure for obtaining the evidence with all information required to identify and procure the evidence. The application has to contain at least one copy in the official language of the requested state and has to be approved by either the Director of Prosecution or the senior most law officer concerned before submitting to the MHA. If the MHA approves the application, the investigating agency can file an LR before a criminal court as envisaged under §166A.

If the court approves the request, the investigating agency must send three copies of the approved request to IPCC and one copy to MHA. The IPCC is the body responsible for sending and follow up on the request in the foreign country. For this purpose, the IPCC works along with the Indian mission at that country. Where there is an existing MLAT or MoU with the requested nation, then the Mission would proceed within the ambit of those documents, in terms of the process and procedure they would follow for future steps. In the absence of such instruments, an assurance of reciprocity is made. If the requested country gives a positive report, the same is forwarded to the investigation agency by the IPCC along with due intimation to the MHA as well as the Ministry of External Affairs. The results of these requests are either sent across in the manner required by the MLAT/MoU or under the usual custom or best practice that is followed internally within a country for such requests.

c) Informal Measures (including Joint Investigations)

There are primarily two less formal methods for access to data across borders . The first is through establishing a MoUs with a country. MoUs, like MLATs provide clarity on the procedure as well as the exact scope of assistance rendered. The difference between MLATs and MoUs are that the latter are not binding. MoUs are usually conceived as precursors to MLATs when, due to diplomatic considerations, it is not

possible to negotiate an MLAT directly. India has such MoUs with Qatar[21], Tajikistan[22] and Bangladesh[23] among others, most of which are over general regional cooperation or cyber security and not just for cross border sharing of data. These MoUs do not necessarily supplement or replace MLATs but are usually broad commitments for specific kinds of crime like fake currency notes, cyberspace, etc.

The second method for less formal access to cross border data sharing is direct procurement of the data from the companies by investigative agencies in India on a case to case basis by issuing a legal request to the company. In the Indian scenario, Section 91 of the CrPC allows a police officer to issue an order seeking production of evidence that is material to an ongoing investigation, which is a separate process and compliance to this request is usually discretionary (at the option of the company) for data stored outside India. However, this approach is limited as some jurisdictions, as noted above, restrict access according to the type of data being requested. For example, the Electronic Communications Privacy Act in the US disallows companies from directly sharing content information of their users with foreign law enforcement agencies and companies thus refer foreign governments to the MLAT process. The companies can disclose this information only if there is a US Federal court warrant to that effect.[24] The European Union also, as a matter of policy, actively discourages direct data sharing without a legal process approved by an institution under the European Union.[25]
For meta and transactional data - companies usually accept legal requests and respond if the request is inline with international law, local law, and company policy.

Companies also usually also consider content, meta and transactional data emergency disclosure requests as well as requests related to joint investigations

21

http://www.mea.gov.in/bilateral-documents.htm?dtl/26869/List_of_MOUsAgreements_signed_during_the_visit_of_Prime_Minister_to_Qatar_June_05_2016

22

http://www.mea.gov.in/bilateral-documents.htm?dtl/27860/List+of+AgreementsMOUs+exchanged+during+the+State+visit+of+President+of+Tajikistan+to+India

23

http://mea.gov.in/bilateral-documents.htm?dtl/25344/List_of_Agreements_MoUs_and_other_Documents_concluded_during_the_visit_of_Prime_Minister_to_Dhaka_June_06_2015

[24] Stored Communications Act 18 USC 2703,

[25] See Maxmillian Schrems v Data Protection Commissioner, EUR-Lex - 62014CJ0362 - EN - EUR-Lex - Europa EU.

where one of the investigating parties is domestic.[26] These emergency requests are accounted for in the ECPA, can be used sparingly and have a very high threshold of preventable, imminent and serious harm that the requester has to demonstrate prior to the request being carried out. Joint investigations, which are usually carried out to counter international syndicated crime networks, also follow a similar process where an informal agreement either bilaterally or via Interpol, lets investigation agencies to share resources, personnel, evidence and data with each other in a cooperative manner. Unfortunately, documentation of joint investigations is not available in the public domain with regard to India as of the writing of this paper.

Differences between Letters Rogatory and MLATs

Having analysed the structure of MLATs and LRs and also having seen their transmission mechanism, it is seen that their transmission methods are more or less the same. The ORF special report released in August, 2017 mentions that MLATs can be initiated directly by the Law Enforcement Agencies without judicial processes while LRs cannot.[27] However it is difficult to reconcile the sending of an MLAT request by an investigation agency without judicial scrutiny since MHA Letter No. 25106/17/201 explicitly requires a cover letter by a court.

It is indisputable however that differences between the both do exist in terms of their scope as well as the compulsion value of the instruments. LRs have a larger scope than MLATs. This is because under MLATs, procurement of only those kind of evidences as permissible by the relevant MLAT and also in the manner as envisaged by the relevant MLAT is possible. Another difference is that while LR procedures mention that a dedicated body, the IPCC will aid with the preparation and transmission of the Requests, no such dedicated bodies exist for MLATs.

However, MLATs compensate for these in a variety of ways.[28] Most importantly, as long as the request is as contemplated under the MLAT, the requested state is obliged under International Law to provide the assistance. No similar compulsion exists on the requested state in the context of LRs. Foreign courts might choose to do so as a matter of comity but this cannot be regarded as an *assurance* of stable

[26] For example, see Google's Legal Process for User Data Requests FAQs. Available at: https://support.google.com/transparencyreport/answer/7381738?hl=en

[27] Bedavyasa Mohanty & Madhulika Srikumar, *Hitting Refresh Making India-US data sharing work* (ORF Special Report, August 2017), p.18.

[28] Margaret K. Lewis, *Mutual Legal Assistance and Extradition: Human Rights Implications* (2 China Rights Forum 2007), p.88.

MLAT Procedure: Issues and Solutions

This infographic attempts to explain the end to end procedure followed for requests under the US-India MLAT from the initiation of the request to the receipt of the information by the requesting party in India. It also highlights key issues faced by the parties at each stage and suggestions solutions to resolve them.

REGULATION CBI Circular/Internal Standing Order		ISSUE	SOLUTION
		Language Legal Awareness Access to Evidence by Defence Nature of Data Legal Threshold Lack of Public Information	Use of Technology (electronic forms, email communication, video conferencing, etc.) Capacity Building Enabling Access to MLAT Requests by Private Entities Mandating Specification of Data Clear legal threshold/standard for MLAT Requests Include model templates, guides, etc. on Central Authority Website
Internal Standing Order	**Ministry of Home Affairs** Internal Security-II Division	Resources Manpower Transparency Judicial Review (esp. L.R)	Allocating additional resources and capacity building Training and expanding workforce Publishing periodical data on MLATs Including review by judicial officer (D.M) prior to forwarding
Internal Standing Order	**Ministry of External Affairs** Consular, Passport and Visa Division	Resources Manpower	Allocating additional resources and capacity building Training and expanding workforce
Internal Standing Order	**Indian Mission** Washington D.C	Manpower Liaison Capacity	Allocating additional resources and capacity building - Training and expanding workforce Dedicated, long term manpower for MLATs.
28 U.S.C. § 1782/18 U.S.C. § 3512	**Office of International Affairs** Department of Justice, USA	Legal Awareness Language	International Co-operation for Capacity Building via cross country training. Electronic Forms and Translation Provisions
18 U.S.C. § 3512/18 U.S.C. § 3512	**Federal Bureau of Investigation**	Manpower	Expanding team to more than 12 members.
18 U.S.C. § 3512/18 U.S.C. § 3512	**U.S Attorney's Office in D.C**	Legal Awareness	International Co-operation for Capacity Building via cross country training.
28 U.S.C. § 1782/18 U.S.C. § 3512	**Federal Court**	Legal Awareness	Dedicated courts for MLAT requests and processing.
Electronic Communications Privacy Act, 1986 + Interception Rules	**Company** U.S	Legal Awareness Manpower Transparency	Internal Capacity Building via Government and Regional Office Cooperation Dedicated, long term manpower for MLATs. Publishing regular and detailed transparency reports.

Disclosure: The content presented in this infographic is a best effort from publicly available information and may not reflect real world practices.

This illustration uses the following icons from the **Noun Project**: Law Book created by **Oliviu Stoian**, Light bulb created by **Numero Uno**, Form created by **Creative Mania**

cooperation.[29] Secondly, MLATs are formal diplomatic channels of cooperation and more systematic and ordered than LRs. The procedures related to each step that are acceptable to both the countries are written down and consequently, there is greater clarity. Since LRs do not have any form of cross country textual backing to support it, such clarity is absent for LRs. For the above reasons, MLATs are more widely used by governments than LRs across the globe.[30]

The India - US MLAT Process

This section will look the the typical laws and regulations that govern the MLAT process by using India and the USA as examples. The goal of the section is to look at the involved government functionaries, understand the nature of internal procedures and finally look at the most prominent problems along with corresponding reforms that can be carried out to make the process more efficient.

India

1) Letter No. 25016/17/2007-Legal Cell of Internal Security Division ('ISD'), MHA [p.2] states that a valid summon, warrant or judicial process[31] has to be given to the ISD along with a covering letter from a court which is essentially the request. The letter also states that if the MLAT treaty allows, the request can be sent directly to the central authority of the requested state without any diplomatic intervention. The India US MLAT does allow this.[32]

USA

1) 28 USC 1782 deals with requests from individuals and LRs.[33] 18 USC 3512 deals solely with MLAT requests.[34]
2) Clause (a)(1) of 18 USC 3512 as well as the official website of the Office of International Affairs ('OIA') of the Department of Justice states that OIA is the central authority which receives and approves requests.

---

[29] L. Song Richardson, *Convicting the Innocent in Transnational Criminal Cases : A Comparative Institutional Analysis Approach to the problem* (26 (1) Berkeley Journal of International Law 62, 2008), p.89.

[30] Bedavyasa Mohanty & Madhulika Srikumar, *Hitting Refresh Making India-US data sharing work* (ORF Special Report, August 2017), p.18.

[31] Valid summons can be issued under Ss. 91, 92, 93, 94, 95, 97 etc of CrPC.

[32] Article 2(3) of the India-US MLAT treaty.

[33] Clause (a), 28 USC 1782; United States Attorney Manual, Criminal Resource Manual 286.

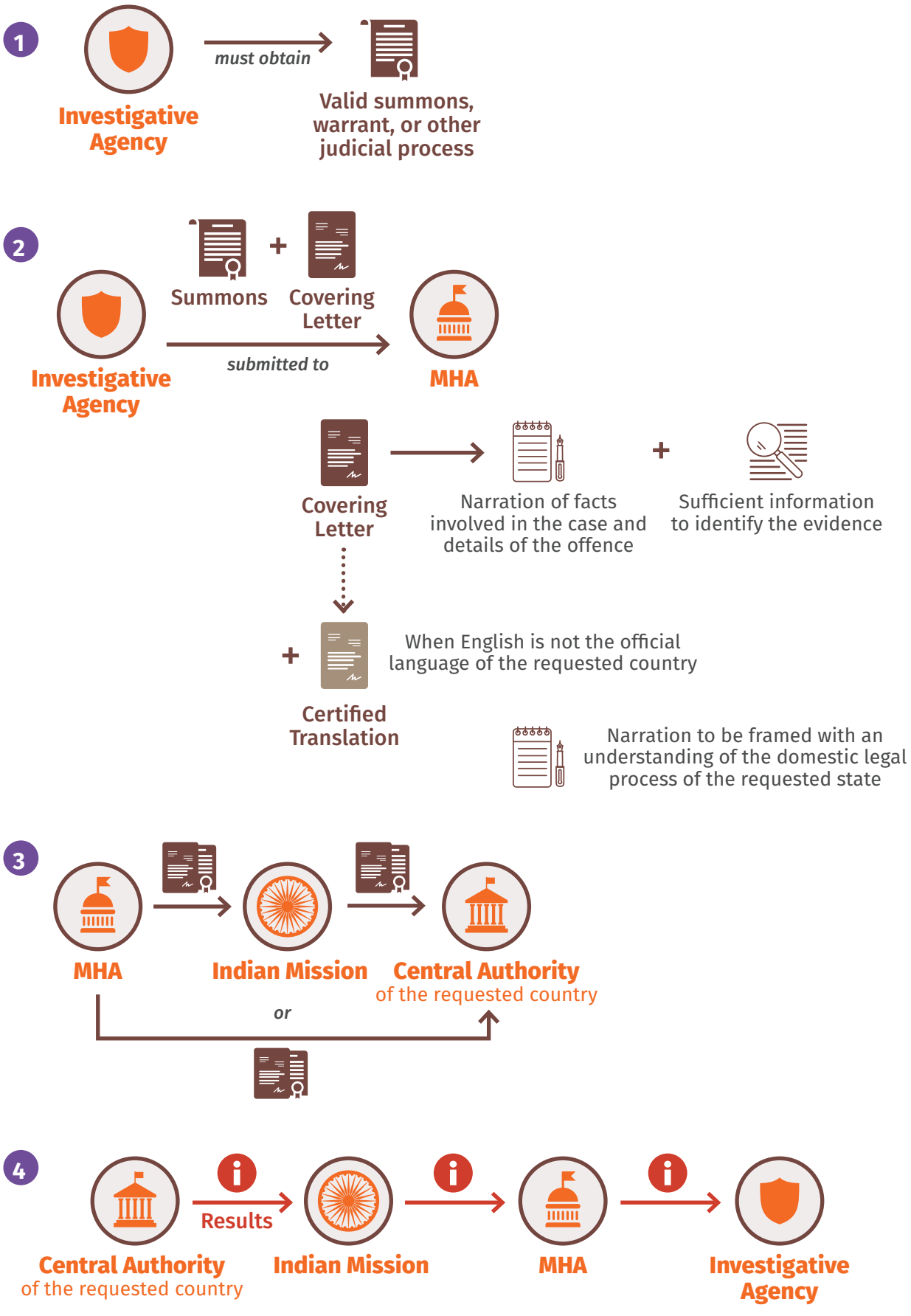
[34] Clause (a)(1), 18 USC 3512.

3) Once approved by OIA, clause (a)(1) of 18 USC 3512 states that the US Attorney of the Court where the request has to go to will have to file the request in court. This is also given in the US Attorney Manual.[35]
4) The court which the request goes to is the Federal Court which has jurisdiction over where the target of the request is located. Multiple legal provisions are applicable here but they all give the jurisdiction as the above itself. Clause (c) of 18 USC 3512 deals with requests in general and fixes jurisdiction thereto. Clause (d) of 18 USC 3512 refers to 18 USC 2703 for requests pertaining to electronic data. Clause (c)(1)(A) of 18 USC 2703 refers to Federal Rules of Criminal Procedure. Rule 41(b)(1) of FRCP fixes jurisdiction as mentioned above.
5) The court gives a warrant which is served on the company which has the data. Clause (a)(1) of 18 USC 3512 as well as clause (a) of 18 USC 2703 are relevant here.
6) According to Article 5(8) of the India-US MLAT, the return chain has to go through the central authorities and cannot be directly from company to investigative agency of requesting state.

b. MLAT Process Flow in the India-USA MLAT (with major issues and tentative solutions)

[35] United States Attorney Manual, Criminal Resource Manual 286.

MLAT Procedure



Letters Rogatory Procedure

1

Investigative Agency → *applies to* → MHA

BEFORE APPLYING

Investigating Officer

- *finds* → Official channels of data sharing between India and the country which houses the evidence; MLATs or MoUs
- *finds* → Any specific requirements for disclosing evidence like dual criminality, or a probable cause standard in the requested country

International Police Corporation Cell (IPCC)

Provides assistance to any investigating officer who may need it

Investigating Officer → Application

- Facts of the case
- English copy of the FIR
- Why the obtainment of such evidence is necessary
- Suggested procedure for obtaining the evidence with all information required to identify and procure the evidence
- At least one copy in the official language of the requested state

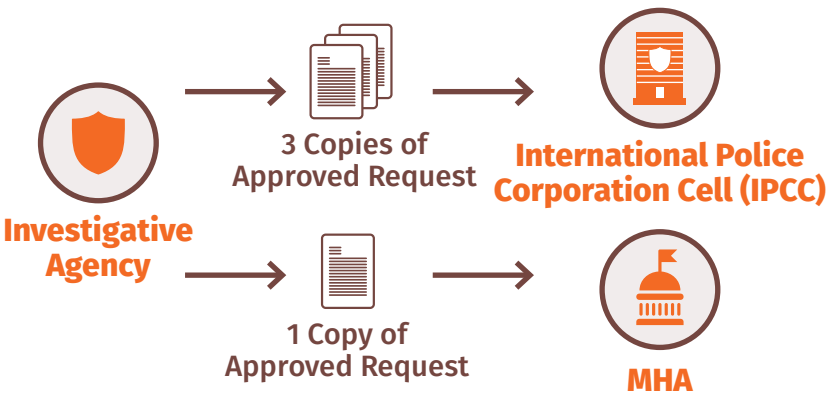
2

Application → To be approved by either the Director of Prosecution or the senior most law officer concerned → *submitted to* → MHA → MHA approved application

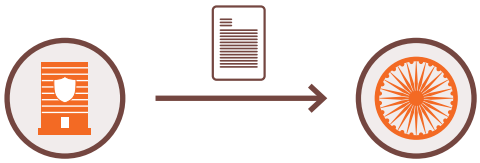
3

Investigative Agency → *files LR to* → Criminal Court

4 ON APPROVAL OF REQUEST



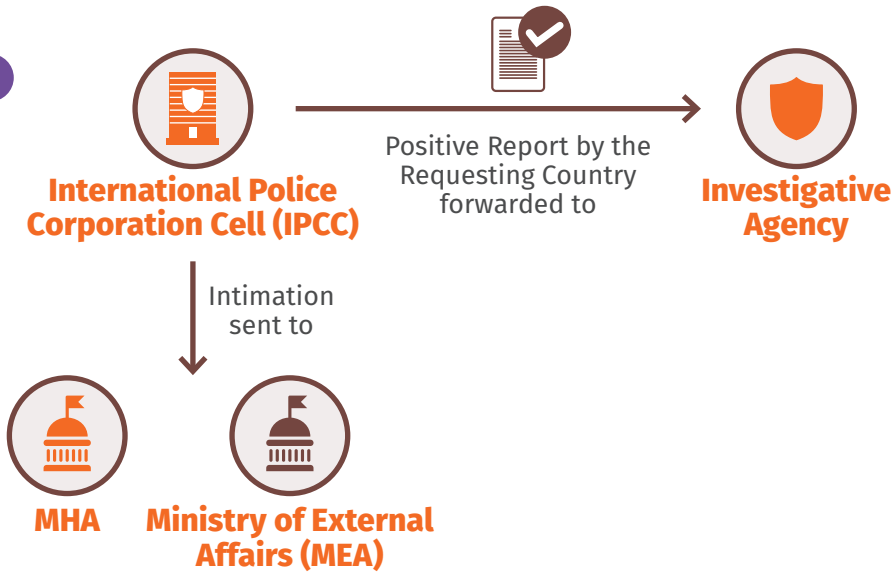
5



Sends and follows up on the request in the foreign country

If there is existing MLAT or MoU with the requested nation, then the Mission would proceed within the ambit of those documents, in terms of the process and procedure they would follow for future steps. In the absence of such instruments, an assurance of reciprocity is made.

6



7

Results

Either sent across in the manner required by the MLAT/MoU

or

Under the usual custom or best practice that is followed internally within a country for such requests

This infographic uses the following icons from the **Noun Project**: Shield created by **Joe Pictos**, Government created by **Rflor**, Police Officer created by **Throwaway Icons**, Court created by **Adricons**, India created by **Anbileru Adaleru,** Warrant created by **Chameleon Design**, Cover Letter created by **Alvarobueno**, Government created by **Adrien Coquet**, Notes created by **Konrad Michalik**, Investigate created by **Made**

Difference Between

LRs

SCOPE
LRs have a larger scope than MLATs

TRANSMISSION OF REQUESTS
LR procedures mention that a dedicated body, the IPCC will aid with the preparation and transmission of the Requests

OBLIGATION FOR ASSISTANCE
No similar compulsion exists on the requested state in the context of LRs. Foreign courts might choose to do so as a matter of comity but this cannot be regarded as an assurance of stable cooperation.

CLARITY OF PROCEDURE
Since LRs do not have any form of cross country textual backing to support it, such clarity is absent for LRs.

MLATs

SCOPE
Under MLATs, procurement of only those kind of evidences as permissible by the relevant MLAT and also in the manner as envisaged by the relevant MLAT is possible.

TRANSMISSION OF REQUESTS
No such dedicated bodies exist for MLATs

OBLIGATION FOR ASSISTANCE
As long as the request is as contemplated under the MLAT, the requested state is obliged under International Law to provide the assistance

CLARITY OF PROCEDURE
MLATs are formal diplomatic channels of cooperation and more systematic and ordered than LRs. The procedures related to each step that are acceptable to both the countries are written down and consequently, there is greater clarity.

For the above reasons, MLATs are more widely used by governments than LRs across the globe.

c. Analysing the India-US MLAT Treaty

Content

India has MLAT treaties with 39 different countries. These agreements differ in scope and requirements.[36] India signed an MLAT treaty with the United States in 2005.[37] The treaty consists of 20 articles and was entered into to improve investigation, prosecution, prevention, and suppression of criminal activity in both jurisdictions. The Articles in the treaty define the scope, terms and process for the collaboration. This section will analyse the India-US MLAT treaty and provide normative suggestions as to how it can be improved to make the MLAT process more efficient and rights respecting.

Scope of Assistance

Presently Article 1 of the India - US MLAT specifies eight forms of assistance:

1. *Taking the testimony or statements of persons;*
2. *Providing documents, records, and items of evidence;*
3. *Locating or identifying persons or items;*
4. *Serving documents;*
5. *Transferring persons in custody for testimony or other purposes:*
6. *Executing requests for searches and seizures;*
7. *Assisting in proceedings related to seizure and forfeiture of assets, restitution, collection of fines; and*
8. *Any other form of assistance not prohibited by the laws of the Requested State.*

To enable effective cross border sharing of data experts have recommended that MLAT agreements specify the forms of communication and data that they cover for example This could include content of digital communications, machine to machine communications, location data, behavioral data, data stored in cloud services, and account data.[38] The India-US MLAT currently does not do this.

The above provision could also be clearer by adopting language in the UN Model MLAT Treaty. Specifically, Article 1 *(c) Effecting service of judicial documents; (f) Providing information and evidentiary items; (g) Providing originals or certified copies*

[36] See: http://www.cbi.gov.in/interpol/mlats.php

[37] http://cbi.nic.in/interpol/mlat/UnitedStatesofAmerica.pdf

[38] Andrew K. Woods, Data Beyond Borders: Mutual Legal Assistance in the Internet Era, Global Network Initiative (January 27, 2015), https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.p

of relevant documents and records, including bank, financial, corporate or business records.[39]

Limitations on Assistance

Article 3 defines four instances of when assistance can be limited:

1. The request relates to an offense under military law that would not be an offense under ordinary criminal law;
2. The execution of the request would prejudice the security or similar essential interests of the Requested State;
3. The request relates to a political offense; or
4. The request is not made in conformity with the Treaty.

Ensuring human rights standards is important in protecting the interests of the citizens of India and foreigners. To achieve this - the treaty could incorporate the language in the model UN MLAT under Article 4 with particular attention to (c) (d) and (e) :

- *(a) "The requested State is of the opinion that the request, if granted, would prejudice its sovereignty, security, public order (ordre public) or other essential public interest;*
- *(b) The offence is regarded by the requested State as being of a political nature;*
- *(c) There are substantial grounds for believing that the request for assistance has been made for the purpose of prosecuting a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions or that that person's position may be prejudiced for any of those reasons;*
- *(d) The request relates to an offence the prosecution of which in the requesting State would be incompatible with the requested State's law on double jeopardy (ne bis in idem);*

(e) The assistance requested requires the requested State to carry out compulsory measures that would be inconsistent with its law and practice had the offence been the subject of investigation or prosecution under its own jurisdiction;"

- **Legality and Necessity:** Section 2 of Article 4 lays down a number of requirements that a request must include:
    - the name of the 'authority conducting the investigation, prosecution, or proceeding to which the request relates;

[39] https://www.unodc.org/pdf/model_treaty_mutual_assistance_criminal_matters.pdf

- a description of the subject matter and nature of the investigation, prosecution, or proceeding, including the specific criminal offenses which relate to the matter;
- a description of the evidence, information, or other assistance sought; and
- a statement of the purpose for which the evidence, information, or other assistance is sought.

The above requirements are predominantly descriptive and lack requirements for the establishment of necessity of evidence requested and a legal basis on which the evidence can be requested. Such requirements are important in ensuring that the MLAT process is not abused to obtain evidence that normally the requesting state would not legally be able to access and in ensuring that the requested evidence is necessary for a legitimate and legally grounded purpose.

Appropriate requirements for data requests

Section 3 of Article 4 requires to the extent necessary and possible. a request shall also include:

a) information on the identity and location of any person from whom evidence is sought;

b) information on the identity and location of a person to be served, that person's relationship to the proceedings, and the manner in which service is to be made;

c) information on the identity and suspected location of a person or item to be located;

d) a precise description of the place or person to be searched and of the items to be seized;

e) a description of the manner in which any testimony or statement is to be taken and recorded; f) a list of questions to be asked of a witness;

g) a description of any particular procedure to be followed in executing the request;

h) information as to the allowances and expenses to which a person asked to appear in the Requesting State will be entitled; and

i) any other information that may be brought to the attention of the Requested State to facilitate its execution of the request.

The above requirements in section 3 do not directly address information that would be necessary to provide for the purpose of accessing data stored by a foreign ICT company. This could include specific accounts, information relating to each account for which records are sought, relevant dates and time spans for requesting the

records, location of the data associated with the account,Internet Protocol (IP) address/website, associated dates and times.

One of the issues experts have identified with the MLAT process is accurate completion of an MLAT request. When an Indian MLAT request is sent to the US it is processed by the Office of International Affairs (OIA). The OIA will confirm that the incoming request is compliant with the terms of the treaty. Once this is confirmed, the request is sent to a federal prosecutor who presents the request to a district court. The court approves or rejects the request based on validity (based on the MLAT treaty and legal standards including probable cause, specificity in warrants, and other human rights) and execution (based on statutory requirements - 28 U.S.C. § 1782 and 18 U.S.C. § 3512).[40] For clarity, these requirements could be included as an appendix to the treaty itself.

Limitations on Use

According to Article 7 *"The Central Authority of the Requested State may request that the Requesting State not use any information or evidence obtained under this Treaty in any investigation, prosecution, or proceeding other than that described in the request without the prior consent of the Central Authority of the Requested State. If the Requested State makes such a request, the Requesting State shall comply with the conditions."*

The limitation on use of information or evidence obtained under the treaty ideally should not be limited to only upon request by the requested state and should be a principle applied by both parties to the treaty on a continuous basis. As an example, the UN model MLAT phrases this as a negative obligation:

"Unless otherwise agreed, the requesting State shall not, without the consent of the requested State, use or transfer information or evidence provided by the requested State for investigations or proceedings other than those stated in the request. However, in cases where the charge is altered, the material provided may be used in so far as the offence, as charged, is an offence in respect of which mutual assistance could be provided under the present Treaty."[41]

[40]Mark Rush and Jared Kephart, "Lifting the Veil on the MLAT process" 20 Jan 2017,"http://m.klgates.com/files/Publication/669681d7-12d7-451e-8240-a33cf67c959f/Presentation/PublicationAttachment/ec5fc22d-3e3c-4607-bcb3-f4e99e3f59b4/GE_Alert_01202017.pdf

[41] https://www.unodc.org/pdf/model_treaty_mutual_assistance_criminal_matters.pdf

Consultation

Article 19 states the *"Central Authorities of the Contracting Parties shall consult, at times mutually agreed to by them, to promote the most effective use of this Treaty. The Central Authorities may also agree on such practical measures as may be necessary to facilitate the implementation of this Treaty."*

This provision could be strengthened through more clear time frames around when and how frequently Central Authorities should meet and could specify that these consultations would include training on each respective jurisdictional requirements for use of the MLAT system. This could be particularly useful as issues around and the need for more clear capacity building on when and how to use the MLAT process has been identified by experts as an area where reform could result in an improved MLAT process.[42]

Key Challenges in the MLAT System

a) Jurisdictional Issues

Various scholars argue that the MLAT process is conceptually flawed and consequently any attempt at reforming it is futile. The strongest argument advanced against MLATs is the impossibility of continuing the location based model under MLATs in light of the technological advancements in the way data is transferred.[43] Google, in its testimony before the Congress, said that its data is constantly in motion along multiple servers located in multiple countries and it might not always be possible to specify the location of the data at any given point in time.[44] Other companies reportedly break down their data into smaller units called shards. These shards can exist in different countries.[45]

---

[42] The Observer Research Foundation has noted: "capacity in the generation and processing of data sharing requests. This capacity deficit is apparent across all institutions responsible for cross-border data sharing. Indian law enforcement agencies do not have adequate training in drafting MLAT requests for data. The institutions tasked with reviewing these requests are often understaffed and ill-equipped to ensure compliance with standards prescribed in the treaty. Despite attempts at institutional reform through personnel training and issuance of circulars, this deficiency in capacity is yet to be addressed." http://cf.orfonline.org/wp-content/uploads/2017/08/MLAT-Book.pdf

[43] Dan Jerker B. Svantesson & Lodewijk Van Zwieten, Law Enforcement Access to Evidence via Direct Contact with Cloud Providers – Identifying the Contours of a Solution (Computer Law & Security Review, 2016), 10.

[44] Written Statement by Richard Littlehale before the United States House of Representatives Committee on the Judiciary Hearing on "Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era", p.4.

[45] Vivek Krishnamurthy, Cloudy with a Conflict of Laws (Research Publication No. 2016-3, The Berkman Center for Internet & Society at Harvard University), Published on February 16, 2016, 4.

For an investigative agency, investigating crime from India, it is almost impossible to find out in which server in which part of the world the specific data is being stored. The concept of shards cause further distortions as a single instance of data can now be stored in parts in different countries. The investigator is then left with no options since he does not know which country to send the MLAT to. However, to be fair to the MLAT system, it must be clarified that MLATs do not conceptually state that the request should be sent to the place where the data is stored. Most of this data is owned by US Companies like Google, Facebook, Microsoft etc. Until a couple of years back, regardless of where the data was stored, these could be accessed by sending an MLAT to the US. However, the US judiciary recently ruled that warrants could not be issued by US judiciary for data existing outside US territory.[46] This ruling has highlighted the complications with a location based system for MLATs.

The tale started in 2013 when a district court judge issued a warrant for the procurement of said data, justifying the acquisition by claiming that Microsoft was an entity incorporated in the United States. Microsoft challenged the legality of this warrant before a Federal magistrate, who held in favour of the United States government. Microsoft appealed this ruling at the United States Court of Appeals for the Second Circuit.

Almost a year before the scheduled verdict, on November 2015, Microsoft chose to matters into its own hands and engaged in a bold manoeuvre that signalled a major victory for the privacy lobby. They came up with an innovative 'data trustee' model where data of all Microsoft's European customers will be stored by T-Systems, which is a subsidiary of Deutsche Telekom.[47] This effectively takes the data out of the reach of the US government as the data is stored entirely on German servers and was taken as a precautionary measure in case Microsoft ended up on the wrong side of the Appeals ruling. The first such 'trustee' facility opened in March of 2016.[48] Deutsche Telekom has also specified that under this model, Microsoft also has no right to

[46] Microsoft v United States, No.14-2985 (2nd Cir. 2016).

[47] https://docs.microsoft.com/en-us/azure/germany/germany-overview-data-trustee

[48] Business Cloud News, "DT keeps data out of US Reach with New Mobility Platform," Business Cloud News March 31 2016,accessed September 10th,2016 < http://www.businesscloudnews.com/2016/05/31/dt-keeps-data-out-of-us-reach-with-new-mobility-platform/>

access the data apart from under exceptional circumstances which is to be determined by Deutsche Telekom.[49]

In the proceedings before the Second Circuit Court , Microsoft premised its arguments on the territorial limits inherent in the concept of a warrant. While the United States authorities certainly had the powers to issue a warrant for the procurement of any material or data within US territory, this power cannot extend overseas unless it is in line with one of the permissive principles of extra-territorial jurisdiction. The Justice Department challenged this ruling in the Supreme Court-a case that was dropped withthepassing of the Clarifying Lawful Use of Overseas Data (CLOUD) Act by the US Congress on March 23rd.[50]

The CLOUD Act states that all service providers are required to disclose data in their posession, custody or control as per lawful processes-regardless of where the data is located.[51] This was the position articulated by the government in the Microsoft-Ireland case. [52]However, the Act crucially adds a new statutory basis that may quash requests on grounds of comity in situations where the US law enforcement authorities attempt to obtain data of a foreigner located extraterritorially and the request generates a conflict with a 'qualifying' foreign government.[53] In these situations, the act requires courts to weigh and balance a number of factors-including the location and nationality of the person, importance of the information to the investigation and the availability of alternative means for timely and effective access.[54]

The second part of the CLOUD Act deals with the converse (and more relevant for India) issue of foreign governments attempting to gain access to data stored on U.S. servers.[55] It seeks to address the problem by providing a mechanism for selected

---

[49] Business Cloud News, "DT keeps data out of US Reach with New Mobility Platform," Business Cloud News March 31 2016,accessed September 10th,2016 < http://www.businesscloudnews.com/2016/05/31/dt-keeps-data-out-of-us-reach-with-new-mobility-platform/>

[50] Greg Stohr, 'Supreme Court drops Microsoft Email with New Law in Place" (Bloomberg,Apr 17,2018) <https://www.bloomberg.com/news/articles/2018-04-17/supreme-court-drops-microsoft-email-fight-with-new-law-in-place>

[51] CLOUD Act § 103(a) (to be codified at 18 U.S.C. § 2703(h)).

[52] Andrew Keane Woods, ' A Primer on Microsoft-Ireland, the Supreme Court's Extra-Territorial Warrant Case" (Lawfare,Oct 16,2017)

[53] CLOUD Act § 103(b) (to be codified at 18 U.S.C. § 2703(h)).

[54] Ibid

[55] Jenifer Daskal, 'Microsoft Ireland,the CLOUD Act and International Lawmaking 2.0'71 Stanford Law Review Online

foreign governments to bypass the MLAT process when investigating a serious crime and directly seek data from US-based service providers pursuant to an executive agreement between the foreign government and the United States provided that the foreign government has satisfied a large number of baseline substantive and procedural requirements.[56]

However, these amendments will not completely solve the issue as powerful international actors like the EU are reluctant to acknowledge the exercise of sovereignty by another country for the data that exists in European soil despite the relevant companies being incorporated outside the EU. The issue of location based jurisdiction will continue to be a huge thorn in the path of MLATs for the considerable future.

b) Delays

Almost all scholars and policy advisers agree that the MLAT process all over the world is plagued with delays.[57] This is also true for India, with an average request taking anything between 10 months to 2 years to be successfully resolved. The primary reason for delays is the sheer volume of MLAT requests that originate today. The staffing within the various departments has not kept pace with the increase in number of requests. However, this is not the sole reason. It is seen very often that the first instance of a request sent is lacking in various important parts that is required under the treaty. Common mistakes include the lack of a consistent legal standard, language errors, incorrectly filled forms and fields, etc.[58] This makes the requested state send back the request and the process has to start again from square one.

c) Lack of Due Process

(2018)https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/04/71-Stan.-L.-Rev.-Online-9-Daskal.pdf accessed July 23rd 2018

[56] CLOUD Act § 105(a) (to be codified at 18 U.S.C. § 2523(b)).

[57] Suzanne Vergnolle, *Understanding the French Criminal Justice System as a tool for reforming international legal cooperation and cross-border data requests* (Georgia Tech Scheller College of Business, Research Paper No. 2017-55), p.215; Gail Kent, *Sharing Investigation-Specific Data with Law Enforcement – an International Approach* (UK National Crime Agency Report, 2014), p.7..

[58] Discussion Paper - what is wrong with the international system for sharing online records for criminal matters?, Access Now? Available at: https://mlat.info/policy-analysis-docs/what-is-wrong-with-the-mlat-system

Most MLATs entered into by India and also most MLATs that exist in the world today explicitly recognize that MLATs can be used only by the prosecution.[59] This is true for the US-India MLAT as well. The disparity in power to adduce evidence blatantly goes against the concept of due process in trials.[60] Further, there are no safeguards in most MLATs to ensure that the evidence procured by the MLAT process is not used by the requesting state in a manner that violates due process of the accused. Thus, the current MLAT frameworks would allow evidence to be used in a trial that may not even follow principles of natural justice.

d) Insufficient Transparency

Transparency is a tool in itself to increase accountability and thereby improve efficiency. There is no information given either on the MHA website or in the CBI website regarding the number of MLAT requests filed, the pending number of requests, which company has been served notice etc. Making such reports available to the civil society increases public scrutiny on the bureaucrats operating the system.[61]

e) Ineffective Privacy

It cannot be denied that privacy concerns and speedy data collection under MLATs are somewhat antithetical to each other. Differences in privacy standards between varying nations are the second biggest thorn in the MLAT process after delays.[62] In the international platform, we see even entities with strong privacy laws like the US and EU struggling to acknowledge that either of them have acceptable privacy norms for faster cross border data sharing.[63] An example of this is the Court of Justice of the European Union invalidating the EU-US safe harbour program, which facilitated faster data sharing, citing privacy concerns.[64] Naturally, the invalidation of this agreement

[59] *See* p.20, Note released by Presidency of the Council of European Union on 25th March, 2011 (available at <http://www.statewatch.org/news/2011/mar/eu-council-eu-usa-mla-handbook-8024-11.pdf>).

[60] Robert J. Currie, *Human Rights and International Mutual Legal Assistance: Resolving the Tension*, p.15.

[61] S*ee* Written Statement by Chris Calabrese before the United States House of Representatives Committee on the Judiciary Hearing on "Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era", p.8.

[62] Cortes, Sarah. "MLAT Jiu-Jitsu and Tor: Mutual legal assistance treaties in surveillance." Rich. JL & Tech. 22 (2015): 1.

[63] Peter Swire & DeBrae Kennedy-Mayo, *How Both the EU and the US are "Stricter" than each Other for the Privacy of Government Requests for Information* (Working Paper Series No. 2017-53, Georgia Tech Scheller College of Business).

[64] Maxmillian Schrems v Data Protection Commissioner, EUR-Lex - 62014CJ0362 - EN - EUR-Lex - Europa EU.

could have had a potentially devastating impact on transatlantic data flows, consequently impacting transatlantic commerce- a relationship that accounts for over 25% of global imports and 30% of global exports.[65] After the commencement of negotiations dedicated to restoring this relationship, in February 2016, the Article 29 Working Party presented the EU-US Privacy shield, which sought to remedy the lacunae in the Safe Harbour Agreement that had been pointed out in the *Schrems* case. [66]

Two major improvements exist in the newly drafted agreement.[67] First, there are now much greater limitations placed on US intelligence agencies and companies in terms of the collection of personal data over the course of intelligence operations. The Office of the Director of National Intelligence assured the EU that "any access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms, preventing generalized access to personal data."[68] Further, The U.S. Department of Commerce will conduct regular reviews on companies that are certified by the Privacy Shield and non-compliance will result in the withdrawal of the certification.[69] The second major improvement is the creation of a formal mechanism of judicial redress for EU citizens who feel that their personal data is being misused or improperly handled. The US government will first create an independent ombudsman under the aegis of the State Department who will follow up with companies regarding complaints made by individual and inform them how the relevant privacy standards are being complied with. Companies are obliged to respond to these complaints within 45 days. If the company fails to take adequate measures, Alternate Dispute Resolution (ADR) mechanisms will be offered free of cost to the concerned individuals. Individuals may also approach their National Data Protection Authorities who will in turn approach the Federal Trade Commission to

---

[65] Joshua Meltzer," Congressional Testimony at Hearing on Examining the EU Safe Harbour Decision and Impact for Translantic Data Flows" (Subcomittee on Commerce, Manufacturing and Trade and Subcommittee on Communications and Technology, United States House of Representatives, Nov,3,2015, Washington DC)

[66] Maximillian Schrems v Data Commissioner (Case-362/14) [2014]

[67] Jemima Kiss, "Privacy Shield lets US Tech Firms Transfer European Data again", The Guardian, 8th July 201accessed 10th September 2016 < https://www.theguardian.com/technology/2016/jul/08/privacy-shield-data-transfer-us-european-union

[68]"Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield (29 Feb,2018)

http://europa.eu/rapid/press-release_IP-16-433_en.htm

[69]European Commission, "European Commission launches EU-US Privacy Shield: Stronger protection for transatlantic data flows," European Commission Press Releases Database,,accessed 10th September,2016 < http://europa.eu/rapid/press-release_IP-16-2461_en.htm

negotiate an acceptable outcome. The Privacy Shield also sets up a mechanism for annual review and policy dialogue with the various stakeholders including consumers, NGOs and corporations. [70]

If the Indian government and the US government were to pursue an arrangement under the CLOUD Act, this agreement would have to be certified by the Attorney-General of the USA that would need to satisfy Section 2523 of the US Code. [71] The certification of this process would require (i) Determining the adequacy of Indian law and the substantive and procedural safeguards for privacy and civil liberties and (ii) an assessment of the provisions of the agreement to ensure they satisfy certain the standards and requirements envisaged in the Act. This must take into account appropriate, credible and expert input. Having in place strong domestic privacy frameworks is increasingly becoming important to the cross border sharing process as proposals that would enable requests for content data to be sent directly to service providers place strong privacy protections as a fundamental criteria to such arrangements.[72]

Secondly, the absence of a privacy code leads to lesser clarity for investigative agencies even while using the existing MLAT processes. For example, the United States has a requirement that any MLAT request coming to it must fulfill the probable cause standard. The absence of any such standard makes it difficult for the Indian investigative agencies to comprehend and therefore fulfill foreign privacy requirements under MLATs.

Solutions & Reforms

Given below is a list of all the solutions and reforms considered in this report arranged according to Content, Capacity, and Process. As their names suggest,

[70]European Commission, "European Commission launches EU-US Privacy Shield: Stronger protection for transatlantic data flows," February 8,2016,European Commission Press Releases Database,,accessed 10th September,2016 < http://europa.eu/rapid/press-release_IP-16-2461_en.htm

[71] See Elonnai Hickok and Vipul Kharbanda " An analysis of the CLOUD Act: Implications for India" https://cis-india.org/internet-governance/files/analysis-of-cloud-act-and-implications-for-india

[72] US Government has drafted the "Legislation to Permit the Secure and Privacy Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism" See: https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p4

content reforms are those which target the content of the treaties;[73] process reforms try to iron out the problems in the physical process of the sending of the treaties; and capacity reforms are those which seek to increase the institutional capacity and add to the knowledge base of those associated with the MLAT process.

a) Effective Due Process

The scholar, Lee Song Richards has written an article on the problem of lack of access to defence in the MLAT process and after a thorough cross comparative analysis of various institutions and mechanisms that could solve this problem, he has concluded that the courts are the best institution to resolve this problem.[74] A change in all existing MLATs to provide for including defense rights to use MLAT processes is much more difficult to actualize than courts mandatorily ordering the prosecution to apply for those evidences on behalf of the defense.

In the Indian context, this translates to mean that either a municipal law should be passed to the effect that mandate prosecutors to apply for evidence on behalf of the accused when requested to do so by him, or the courts themselves must impose this obligation on the prosecution citing natural justice principles. Natural justice principles allow a person an opportunity to present his case. The spirit of this principle would be lost if the defendant is barred from adducing evidence to effectively present his case. In most cases, the defendant would have access to his/her own data either directly or through a request directed at the foreign company on whose servers the data is stored. The question becomes more complicated when a data belonging to a non-citizen is critical for establishing the defendant's claims. For instance, a *Microsoft-Ireland* like situation may arise where the data stored on foreign servers is not needed by the prosecution but by the defendant as vital evidence.

Another perspective to protecting due process within the MLAT framework is by making sure that no assistance is provided by India in a manner that violates due process of any person regardless of her nationality. To achieve this, various clauses have to be incorporated in the treaty itself. Firstly, it must be ensured that requesting states are bound by the MLAT treaty to provide a fair trial to any person against

[73] Importance of content reforms have been highlighted in the Global Network Initiative Report on *Data Beyond Borders Mutual Legal Assistance in the Digital Age*, p.13 (Andrew K Woods, January 2015).

[74] L. Song Richardson, *Convicting the Innocent in Transnational Criminal Cases : A Comparative Institutional Analysis Approach to the problem* (26 (1) Berkeley Journal of International Law 62, 2008).

whom this evidence is being used. The parameters of such fair trial, which include *audi alteram partem*, and *nemo in propria causa judex esse debet* should be specified in the treaty itself. Secondly, there should be a provision for refusing assistance if it is found that the request is made for punishing a person solely for that person's race, sex, religion, nationality, ethnic origin or political opinions.[75] Thirdly, there must be an explicit clause which allows refusal of assistance on grounds of double jeopardy.[76]

b) Improving Privacy and Transparency

The reform to the problem of international privacy considerations hampering investigative efforts is straightforward. The parliament must enact a comprehensive privacy protection code. The domestic conditions for the same are ideal after the verdict of the Supreme Court in *KS Puttaswamy*[77] recognizing privacy as a Fundamental Right in India. While drafting this legislation, care has to be taken to conform to international standards as much as possible. It is imperative that we take the privacy concerns of at least the countries with a larger share in the IT market into consideration while drafting the privacy legislation in order to protect the efficiency of cross border data sharing for India. An example of such a concern raised by the EU is that the municipal legislation in a country must not restrict the scope of their privacy rights to their own citizens and EU citizens should also be protected thereto.[78]

Solving the problem of lack of privacy protections within MLATs require actual changes to the clauses in the various MLATs we enter to. It is suggested that India push for clauses in its treaties which mandate that the facts and circumstances that led to the request for evidence, should satisfy the principles of necessity and proportionality. There should also be clauses in the treaty that define in clear terms, the threshold for necessity as well as proportionality so that there is no confusion for investigative agencies. Another clause that helps in the interest of privacy is mandating that communication through MLAT processes if through digital forms should be encrypted.

---

[75] Such a provision is found in Article 4 (c) of the Model UN MLAT treaty, available at < https://www.unodc .org/pdf/model_treaty_mutual_assistance_criminal_matters.pdf>

[76] Such a provision is found in Article 4 (d) of the Model UN MLAT treaty, available at < https://www.unodc .org/pdf/model_treaty_mutual_assistance_criminal_matters.pdf>

[77] Justice K.S. Puttaswamy v Union of India, Writ Petition (Civil) No. 494 of 2012.

[78] Paolo Balboni & Enrico Pelino, *Law Enforcement Agencies' activities in the cloud environment: a European legal perspective* (Information & Communications Technology Law 22(2) 2013), p.167.

c) Solutions to Jurisdictional Issues and Delays

Since, this problem is entrenched with the very nature of MLATs, reforms thereto exist as alternates to the MLAT process itself. There are two such alternates. The first method questions the very legitimacy of blocking provisions like the Stored Communication Act ('SCA') in the US and the dozens of EU regulations that disallow companies from responding to foreign requests.[79] This line of argument criticizes the blatant paternalism being showcased by these countries.[80] The argument states that the investigation of offences that take place within the territory of a country should be left to that country. Impeding the efficiency of this investigation citing privacy concerns especially when its own citizens are not involved is mere abuse of a dominant position that these countries hold in the IT industry at the moment.

Following this conception of international cooperation, the entire problem of data sharing will be overcome. An investigation agency in India would only need to acquire a summons as it would for any Indian company that stores its data within India. The company would respond to the legal process or risk facing proceedings in Indian courts. This method also solves the problem of location based jurisdiction as now the jurisdiction is based on whether the state has a legitimate interest in seeking the information. A concern with this approach is the potential negation of privacy in this paradigm as well as confidence that requests have been accurately and fairly evaluated and complied with by companies. Privacy is now considered by various international instruments as a Fundamental Right.[81]

The second method is for creation of direct data sharing agreements not as a matter of right but based on consent of various nations. Thus, if India has a direct sharing agreement with the US, because of the consent provided by US when entering into the contract, Indian courts would be able to send the warrants directly to US companies premised on this agreement. An example of such an agreement existing currently is the European Investigation Order ('EIO'). Under this treaty, EU countries

[79] *Data & Jurisdiction Program: Cross-Border Access to User Data* (Internet & Jurisdiction Report, May 2017), p.6.

[80] Written Statement by Prof. Keane Andrew Woods before the United States House of Representatives Committee on the Judiciary Hearing on "Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era", p.7.

[81] Paolo Balboni & Enrico Pelino, *Law Enforcement Agencies' activities in the cloud environment: a European legal perspective* (Information & Communications Technology Law 22(2) 2013), p.168.

agree to recognize court orders from other member countries for investigative purposes as operable within their territory.[82]

Another major direct data sharing agreement down the pipeline is the proposed US-UK direct data sharing agreement.[83] This agreement is limited to data sharing but otherwise works in a similar manner as the EIO. The best way to understand the direct sharing agreement is to compare it with the US Visa Waiver Program.[84] In that program, countries were ranked according to their quality in Visa related laws and there were various relaxations given to those countries which scored high in the ranking provided there was reciprocity. The direct sharing agreement does the same thing by looking at a number of factors include the strength of privacy and civil liberties protections in a foreign country. As a part of this, the blocking provision of the SCA will be relaxed for countries that are determined to have acceptable frameworks and protections in place. The specific protections to be given in order to avail of this relaxation have already been conceptualized by the Justice Department in the US. Consequently, if India wishes to participate in the envisioned system, it is imperative that India enact a robust privacy protection code.

➔ **Process Reforms**

- Improving the funding for MLAT process.
- Recruiting more staff in the Internal Security Division II of MHA.
- Set individual deadlines for all domestic departments dealing with MLATs.
- Create a web based portal where requests are uploaded by the investigating agency and the status of the request can be checked on a real time basis.
- Employ liaisons in requested countries (at least the important ones like US) whose sole job is to expedite MLAT requests.
- Employ liaisons in the MHA for each separate state so that investigative agencies have a state specific person to help them with framing requests and getting their requests approved.
- Release public reports with statistics regarding the number of requests filed, number of successful requests, reasons for failure etc.

[82] European Investigation Order, DIRECTIVE 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 3rd April 2014

[83] Written Statement by Paddy McGuinness before the United States House of Representatives Committee on the Judiciary Hearing on "Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era".

[84] Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program* (71 NYU Annual Survey of American Law 687 (2017)).

- Have a privacy law passed consistent with international best practices.
- Negotiate direct data sharing agreement with countries.
- Provide access for defence within the MLAT framework.
- Negotiate with countries having a high concentration of MLAT requests like the US to have specialized tribunals to deal with MLATs rather than putting it in a usual federal court docket.
- Push for provisions in MLATs which explicitly allow sending of messages over expedited and secure channels like encrypted electronic mail rather than mail. Push also for digitizing the entire MLAT process through web based portals.

➔ **Capacity Building and Educational Reforms**

- Post model templates online for each country with which India has an MLAT so that investigation agencies are familiar with the requirements while drafting requests.
- Give periodic training to investigative agencies as well as the MHA personnel involved in transmission of MLATs so that they are familiar with the requirements of MLATs.
- Have a dedicated department for helping investigative agencies with framing MLAT requests similar to the International Police Cooperation Cell for LRs.
- Organize annual conferences with representatives from all countries with which India has MLATs so that difficulties from their end can be discussed and ironed out.

➔ **Content Reforms**

- Push for clauses in MLATs which state that a request will not be invalidated on account of lack of information provided that there is enough information to identify and acquire the evidence sought for.
- Have clauses specifically which allows expedited testimony collection like video conferencing.
- Have clauses which allow easy transfer of data related to bank details.
- Have clauses which protect due process considerations like audi alteram partem, double jeopardy, vindictive prosecution etc.
- In the interest of privacy, ensure that the MLAT obliges the requesting state to disclose the necessity of procuring the information and how the same is proportional to the invasion of privacy sought.

- Provide clauses which envisage time bound consultation between the Central authorities so that difficulties are resolved instead of the request remaining at a standstill / being rejected.
- **Access to Evidence by the Defense:** The US-India MLAT does not provide the defense access to evidence. This practice is not common in MLAT agreements but is found in the US MLAT agreements with Switzerland, Turkey, and the Netherlands.[85]
- **Procedural and Substantive Rights**: It is important that the rights of individuals are protected and upheld in the process of cross border sharing of data for criminal purposes. This can be ensured by including the right to a fair trial, the right to an effective remedy. Substantive rights - namely privacy, can be upheld by incorporating the principles of necessity, proportionality, legality, legitimate aim, adequacy, and transparency.[86]
- **Consistency with ICCPR:** The MLAT agreement could incorporate the safeguards and standards found in the ICCPR as a baseline for protecting human rights in the cross-border data sharing process.
- **Utilise principles of International Law as a baseline tool for negotiations:** Despite the uncertainty in the hierarchy of various permissive principles for extra-territorial jurisdiction, it is clear that Indian jurisprudence recognises these principles. International Law dictates that the hierarchy would need to be determined based on which country has a greater substantial connection to the rime at hand when deciding a conflicts situation. between a country, which is merely storing data as the processor is a company incorporated there and a country where the crime has been committed or whose citizens have been affected, it is clear that the latter would have a more substantive connection. Echoing these principles either in the MLAT agreement or any agreements entered into under the CLOUD Act should reflect this hierarchy. The argument can be made more cogently if these principles are referred to during the negotiations.

[85] http://m.klgates.com/files/Publication/669681d7-12d7-451e-8240-a33cf67c959f/Presentation/PublicationAttachment/ec5fc22d-3e3c-4607-bcb3-f4e99e3f59b4/GE_Alert_01202017.pdf

[86] These principles have been defined and articulated in the Necessary and Proportionate principles. See: https://necessaryandproportionate.org/principles

Conclusion

This report analyzed literature surrounding MLATs to identify the necessity for having efficient MLATs, how MLATs and LRs operate in India, problems faced by MLATs, solutions thereto, and alternate data sharing systems. In the light of the importance of having an efficient MLAT system and the complexities involved in achieving this, it is suggested that the Parliament pass an MLAT act. Various Countries like South Africa,[87] Canada,[88] and United Kingdom[89] have already passed such Acts. In addition to this statute, India needs to think of an enabling ecosystem that starts with a high-level policy framework which sets the tone for diplomatic negotiations that would affirm India's position when negotiating it's position in the CLOUD Act determined pecking order. This framework needs to be underscored by robust safeguards and protection in India along with a clear articulation of India's incorporation on international principles on extra-territorial jurisdiction. While proposed data localisation measures may change the landscape, it is imperative that any measures are enforced through diplomacy and consultation with other stakeholders in the system.International Law was designed to serve as a common baseline that could enable pragmatic negotiations and despite the inherent ambiguities in the understanding of jurisdiction in international law, a cogent articulation of the permissive principles would enable India to ascertain it's position more clearly and in the age of deals, strike a better one for itself. As the nature of policing changes to a model that increasingly relies on electronic evidence, India needs to ensure that it's technical strides made in accessing this evidence is not held back by the lack of an enabling policy environment.

---

[87] International Cooperation in Criminal Matters Act, 1996; For more information on the Act, *see* Murdoch Watney, *A South African Perspective on Mutual Legal Assistance and Extradition in a Globalized World* (Potchefstroom Electronic Law Journal 15(2) 2012).

[88] Canada (Mutual Legal Assitance Act); For more information on the Act, *see* Julian M. Joshua, Peter D. Camesasca, & Youngjin Jung, Extradition and Mutual Legal Assistance Treaties: Cartel Enforcement's Global Reach (Antitrust Law Journal 75(2) 2008), p.43.

[89] UK (Crime International Cooperation Act), 2003; For more information on the Act, *see* Julian M. Joshua, Peter D. Camesasca, & Youngjin Jung, Extradition and Mutual Legal Assistance Treaties: Cartel Enforcement's Global Reach (Antitrust Law Journal 75(2) 2008), p.43.