

## Hitting Refresh

MAKING INDIA-US DATA SHARING WORK

BEDAVYASA MOHANTY & MADHULIKA SRIKUMAR

# Hitting Refresh

---

MAKING INDIA-US DATA SHARING WORK

BEDAVYASA MOHANTY & MADHULIKA SRIKUMAR

Hitting Refresh: Making India-US Data Sharing Work  
Authors: Bedavyasa Mohanty and Madhulika Srikumar

© 2017 Observer Research Foundation. All rights reserved.

### **Acknowledgements**

The authors would like to express their sincere gratitude towards the law enforcement officials, industry representatives and policymakers for their invaluable time and guidance for this paper. The authors would also like to thank the reviewers for their comments on earlier drafts of the paper; in particular, thanks are due to Vinia Datinginoo Mukherjee for her incredible patience and timely editorial inputs. This paper would not have been possible without the support of Google. While several stakeholder inputs were taken in the course of writing this paper, all views expressed here as well as errors therein are the authors' alone.

**Designed by:** Ashwin Karupaiah

**Printed by:** Vinset Advertising, New Delhi

Observer Research Foundation (ORF) is a public policy think-tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research, and stimulating discussions.



To know more about  
ORF scan this code

# Contents

<b>Executive Summary</b>	1
<b>Introduction</b>	5
<b>Treatment of Data</b>	
• <b>Types of Data</b>	10
• <b>Company Practice</b>	11
<b>Data Requests</b>	
• <b>Investigation in India</b>	
<i>Collection of evidence</i>	14
<i>Admissibility of evidence</i>	14
• <b>Direct Requests</b>	
<i>When LEAs request non-content data from US companies</i>	15
<i>When LEAs make emergency requests to US companies</i>	16
<i>When LEAs make data preservation requests</i>	16
• <b>Formal Requests</b>	
<i>MLATs v. Letters Rogatory</i>	17
<i>India-US MLAT</i>	18
<i>India side of the process</i>	20
<i>US side of the process</i>	21
<i>Letters Rogatory</i>	22
<b>Key Takeaways</b>	24
<b>Short Term Reforms</b>	
• <b>For Companies</b>	28
• <b>For Law enforcement</b>	28
• <b>For Policy Makers</b>	29
<b>Long Term Reforms</b>	
• <b>Direct Data Sharing as an Alternative to MLAT</b>	32
<b>Conclusion</b>	37
<b>Appendix</b>	40
<b>Endnotes</b>	45





# Executive Summary

Commentators have long agreed that the system for cross-border sharing of data for criminal investigations under Mutual Legal Assistance Treaties (MLATs) is broken. During a consultation held by the Observer Research Foundation(ORF) on India-US data sharing, officers of Indian Law Enforcement Agencies (LEAs) echoed this opinion, calling the MLAT system not only broken but “beyond repair”. Others have not had such a dire view and see the MLAT process as an important tool, but all acknowledge that the MLATs alone cannot handle the volume of legitimate requests for electronic data held by foreign companies. Over the past decade, access to electronic data has become instrumental to further investigations not just for crimes online but also for criminal activities in the physical domain. Most companies that offer widely used email and social media platforms are incorporated in the US and are subject to US law that can restrict to whom and under what circumstances they may disclose data they hold, regardless of where the user is located.

The system governing user data sharing between communications service providers and investigating agencies is for a lack of a better term, a stopgap one. The primary means available to investigating officers to access data of Indian users held by non-Indian companies are requests through the MLAT process or letters rogatory and direct requests. The MLAT process, however, was not conceived for meeting electronic data requests from foreign law enforcement agents.

The practice that American companies follow when responding to direct requests from foreign law enforcement agencies is one that has evolved over time and is carried out voluntarily by companies, who are subject to the restrictions under US law. The governing statute for law enforcement access to user data, the Stored Communications Act (SCA), is a law from the 1980s that did not account for the law enforcement needs of other countries. Through permissive interpretation, companies have been able, consistent with the SCA, to disclose non-content data voluntarily to government agencies in jurisdictions that honor the rule of law and respect fundamental human rights. Companies during exigent circumstances involving danger of death or serious physical injury to any person also voluntarily reveal data to Indian law enforcement agents.

On the other hand, for revealing content of communications to foreign governments, the SCA requires companies to comply with a warrant issued in the US. As a result, in most cases investigating officers in India must obtain a warrant meeting the probable cause standard from a US court through the India-US MLAT to access content data. As the primary mode of obtaining content data, inefficiencies in the MLAT process continue to be heavily criticized.

MLATs are diplomatic agreements entered into between states to exchange evidence for criminal investigations and prosecutions. The India-US MLAT that came into force in 2001 enabled both countries to provide assistance in extraordinary circumstances such as cases of terrorism or economic crimes. The sharing of electronic data under the MLAT however is a long-winded, time

consuming and laborious process for Indian and US law enforcement agencies. The mechanism of evidence sharing under the treaty was not built to handle the volume of requests for electronic data that is now commonplace in the digital age.

The authors of this paper during their interviews discovered that the pending requests under the India-US MLAT number only in the hundreds, of which some concern electronic data. This number however is not indicative of the demand for electronic data during criminal investigations as several officers are discouraged from making MLAT requests in the first place owing to the procedural delays and complexities involved. As a police officer noted during the ORF consultation, the number of requests that Indian law enforcement agencies make to telecom service providers for interception and access to data is more indicative of law enforcement requirement for data than requests to American companies.

With users, companies and data located across different jurisdictions, investigating agencies and companies often have to navigate a minefield of conflicting laws and procedures to access data and respond to requests. This has resulted in states either calling for data to be localised within their borders<sup>1</sup>, enforcement agencies using other means to access data disregarding user privacy<sup>2</sup> or courts applying domestic laws beyond their borders to access data of their citizens<sup>3</sup>.

There is an appetite amongst policymakers and law enforcement agencies in India to find for alternatives to the MLAT mechanism. Many US providers share this outlook. During the consultation, a discussant remarked that discussing inefficiencies under the MLAT would serve little purpose, as it is now well established that electronic data sharing is ill served by the current system. Indian stakeholders are keen for the respective governments to consider a data sharing agreement similar to the one currently being negotiated between the UK and US. This data sharing agreement would enable Indian agencies to make requests directly to US companies for content and real-time data – no longer making access to user data or safeguards against it subject to US laws.

To enable such data sharing, the US Department of Justice (DoJ) in 2016 introduced amendments to the Electronic Communications Privacy Act (ECPA) removing the federal warrant requirement for foreign requests. The ECPA amendment if passed would require the signing country to offer substantial privacy protections addressing access, storage and review of data. Policymakers during interviews for this paper recognised this as an opportunity to have Indian laws scrutinised and reformed. These reforms will need to include higher safeguards during access of data, institution of judicial review of data requests and increased transparency around interception orders.

The Indian government is in the process of re-examining existing laws and is framing a new legislation. A ten member expert committee has been constituted to introduce a new data



protection Bill<sup>4</sup>. With a nine judge constitutional bench of the Supreme Court currently deciding whether Indian citizens enjoy a fundamental right to privacy – an overhaul of India’s data protection framework may be on the cards. These changes will act as an impetus for the India and US governments to push through a direct data sharing agreement to find an alternative to the MLAT process.

Meanwhile in the short term, law enforcement agencies, companies and policymakers must undertake reforms to improve the process for cross border data sharing under the India-US MLAT. US companies should increase transparency around reporting of data requests. Indian law enforcement agencies on the other hand must build capacity within state and central agencies, institutionalizing inter-agency cooperation. Officers should be trained to be clear and specific in drafting requests. The Ministry of Home Affairs (MHA) should also build capacity and expertise to receive and review requests, establishing a dedicated team of legal officers trained in international criminal law and law enforcement agents on deputation. The MLAT process can be significantly transformed if it is digitized, requests for supplementary information are streamlined and internal time limits are introduced.

This paper is not the first of its kind. While there exists significant literature chronicling problems with the MLAT process, there is little that examines this problem through an Indian lens. This paper aided by interviews with Indian investigating agencies, policymakers and electronic communication service providers, has attempted to identify elements in the data sharing process that result in inefficiencies. It also suggests reforms that can help address these inefficiencies – both in the short and the long run.



# Introduction

The massive shift to online communications services in the last decade has brought unprecedented benefits. States that have provided open access to the internet have successfully spurred their digital economies forward and bolstered civil liberties. Among emerging economies, India boasts a significant and growing online population as the country undergoes a rapid digital transformation propelled by the Government's Digital India Initiative. With nearly 450 million Internet users, India is a critical market for some of the most successful startups in recent memory: Facebook<sup>5</sup>, Whatsapp<sup>6</sup> and UBER<sup>7</sup>. Spawned in Silicon Valley alongside other internet companies from the 1990s – these companies host a sizeable portion of the world's data<sup>8</sup>. As a net exporter of data, accessing this information for lawful investigation presents a challenge for India. Even in instances where crimes occur within a sovereign state's territory and both the accused and victim are citizens of the state – law enforcement agencies (LEAs) find it difficult to expedite investigations owing to difficulties in obtaining lawful access to data of foreign providers.

Investigation and prosecution of crime has always been the sovereign prerogative of a state. This prerogative was closely linked to the territorial control that a state exercised. 20th century institutions to manage global trade, tackle trans-national terrorism, and protect international human rights have all sought to de-couple a country's sovereign responsibilities from the territory it controls, but none have had the visible effect of eroding sovereign capacity as the emergence of electronic communication and cross-border data flows<sup>9</sup>. Nevertheless, law enforcement remains the prerogative of the state alone. With the rise in criminal investigations involving electronic evidence and crimes in cyberspace costing the global economy \$445 billion a year<sup>10</sup>, the need for inter-state cooperation to tackle these crimes has heightened.

To obtain evidence across territorial borders, governments typically rely on diplomatic procedures, such as formal bilateral or multilateral instruments or else turn to informal channels of government-to-government cooperation. Central among these formal arrangements are Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory – which allow law enforcement agencies to obtain data stored by Communications Service Providers (CSPs) abroad. The internet's centrality to routine communications and the advent of cloud storage has all but ensured the primacy of electronic data to any criminal investigation. The efficacy of MLATs however has often been called into question<sup>11</sup>, largely due to the lengthy and labour intensive processes involved – systemic problems that have only exacerbated under increasing requests for user data.

The underlying structure of MLATs, however, remains vital and represents the best way for countries to identify and address competing equities. The MLAT process allows one country to request information held by a provider in another country, thus addressing that country's important equity to pursue an investigation, and allowing the government of that other country to ensure that the companies within its jurisdiction are acting appropriately in disclosing user data.

The challenge with MLATs for sharing electronic data comes not from its underlying premise, but in execution. MLATs were conceived for sharing evidence during exceptional circumstances and are ill suited for the volume of electronic data requests that are now commonplace. Indian law enforcement agents (LEAs) at the state and central levels often bemoan the fact that the difficulty in obtaining data from providers located in the US makes the prospect of filing an MLAT request an unattractive proposition. Indian LEAs also find that making direct requests to service providers is an unreliable option as company practices are often found to be opaque. Despite multiple attempts at international cooperation and diplomacy between the two nations, no clear solutions to the data-sharing conundrum have emerged. The Framework for U.S-India Cyber Relationship<sup>12</sup> highlighted the need for increased cooperation between law enforcement for investigating cyber crime as well as the need for real time data sharing for cyber-security. In spite of cooperation on cyber crime investigation being a central consideration for both governments in recent years, there has not been any significant headway in bilateral data sharing processes.

The differential treatment of data in law and practice in India and the US have added to the challenges faced by Indian law enforcement in accessing data. LEAs also perceive many company policies on responding to requests from foreign governments as inconsistent and unclear, often frustrating well-established procedures in domestic criminal investigations. Cumbersome and outdated processes found in the requesting and requested states further complicate requests for user data under formal channels like MLATs or Letters Rogatory. One way of harmonising conflicting laws regarding data access is by making law enforcement access to data not contingent upon the location of the data or the CSP but the location and nationality of the user. A bilateral data sharing agreement similar to the one being contemplated by the US and UK would make access to data subject to the laws of the requesting state when the crime is serious in nature. Under such an agreement a foreign law enforcement would be able to make a direct request for data from a CSP located abroad. This is not to say, however, that a data sharing agreement is a silver bullet that can solve all problems. Direct data sharing throws up many more challenges in the form of potential privacy violations. Therefore, a data sharing agreement must be complemented by strong domestic laws and regulations that provide robust privacy protections – as rigorous as the US probable cause standard.

This paper, through interviews with law enforcement agencies, representatives of electronic communication service providers, government officials and judges, attempts to dissect the current procedure for data requests made by Indian law enforcement agencies. The first part of the paper addresses the different kinds of data that communication companies store and the practices that companies follow when revealing data to foreign law enforcement agencies.

The second part addresses how an investigation is carried out in India to set the context of law enforcement needs for this data. This part further lays out practices of Indian law enforcement agencies in accessing content and non-content data – deconstructing the procedure followed for making requests either directly to the company or under an MLAT or Letters Rogatory. It attempts

to clarify this process, beginning from the time that a law enforcement makes the request for information to the time that an American company provides the data. The third part identifies key takeaways from the Authors' research and interviews with law enforcement agents and industry representatives. The fifth part suggests reforms that American companies and law enforcement agents in India can undertake to streamline data requests in the short term. The fourth part examines a bilateral data sharing agreement as an alternative to the MLAT process. This paper restricts its scope to data requests made to companies incorporated in the US, consequently only addresses the problems associated with the India-US MLAT.



# Treatment of Data

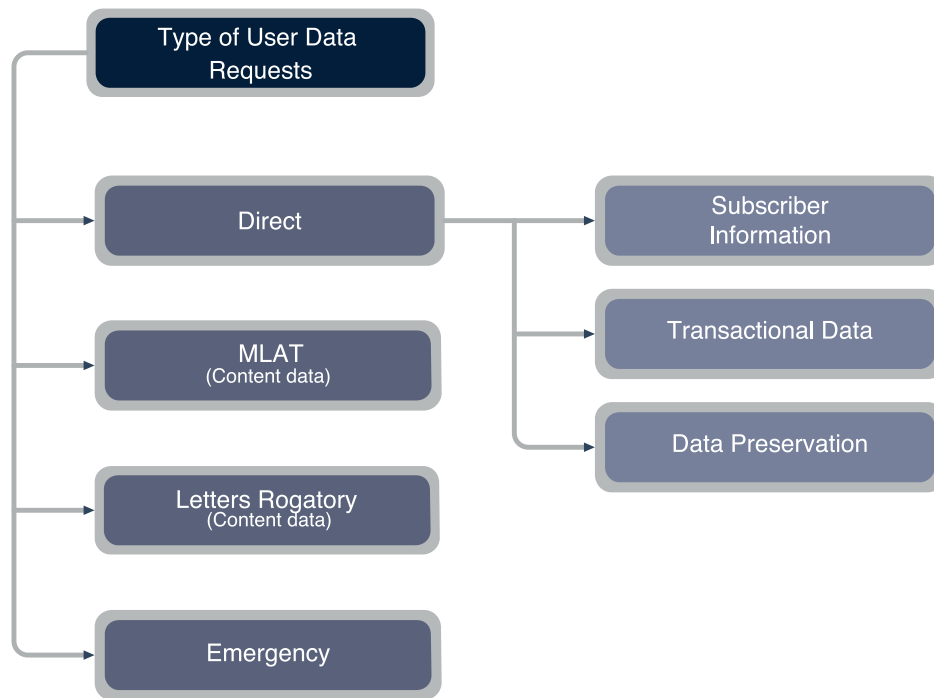
US law refers to three types of user data, which is reflected in the company policies and transparency reports of many US providers: ‘basic subscriber information’ (BSI) which is data provided by a user at the time of registration or sign-up and typically includes IP addresses associated with logins to the service, ‘other records’ (more commonly referred to as ‘transactional data’) which is the information related to the communication (like email headers, or IP addresses used to upload content like a photo, or to send a communication like an email) and ‘content data’ which is the substance, purport or meaning of a communication<sup>13, 14</sup>. Subscriber information and transactional data are collectively understood as metadata or non-content data.

## Types of Data

Subscriber information is typically data provided by users at the time of creating an account with an online service. The ECPA specifically lists the types of data that fall in this category. Examples of subscriber data include name, associated email address, phone number and payment details, and the aforesaid IP addresses. Transactional data is information relating to the senders and recipients of a communication and includes data on the origin, destination, time, route and size of the message. In some contexts, metadata can include geolocation information and device-specific information<sup>15</sup>.

In the internet age, the distinction between metadata and content data may not always be apparent. Metadata if properly analyzed can be as revealing as content data, if not more. It is for this reason that the traditional analogy of metadata resembling the address found on an envelope and content data resembling the letter in an envelope, is imperfect.<sup>16</sup>

Content data refers to the substance, purport or meaning of the communication which can either be in transit or stored on the user’s device and/or the service provider’s servers. Communications content these days is often encrypted both during transit and in rest.<sup>17</sup> Examples of content data include email content, communications over VoIP services and exchanges over instant messaging applications. The standards for obtaining content are more stringent than that of metadata in most jurisdictions<sup>18</sup>. This is because content of communications is often considered more private than non-content and carries with it an enhanced expectation of privacy among users.



*Fig. 1: Types of Requests that US communication service providers receive from Indian LEAs*

## Company Practice

The type of data requested by an LEA officer determines what procedure he/she will have to follow to obtain user data from a communication service provider. Companies collect data from users that can be broadly divided into the aforementioned kinds – subscriber, transactional and content.<sup>19</sup> Companies, incorporated in the US are subject to the ECPA, that regulates standards of law enforcement access to customer data.<sup>20</sup> The ECPA consists of three statutes, the Stored Communications Act (SCA), the Wiretap Act and the Pen Register statute.<sup>21</sup> The SCA covers access to stored, content and non-content data while the Wiretap Act and Pen Register statute address real time access to data by LEAs.

Direct requests are those where foreign governments or law enforcement agencies can request data from communication service providers located in the US without relying on any US legal process.<sup>22</sup> It is a voluntarily developed industry practice to disclose non-content data to foreign governments on receiving a data request even in the absence of a US legal order.<sup>23</sup> Companies are able to do so as the ECPA only prohibits voluntary disclosure of non –content data without valid legal process to US government entities and not foreign governments.<sup>24</sup>

Following a Sixth Circuit ruling in 2010<sup>25</sup> that held that “content” is protected by the Fourth



Amendment in the US Constitution, most major companies furnish content data to governments only when issued a search warrant by a competent US court.<sup>26</sup> Companies apply the same policy to requests for content data from foreign governments that are routed through MLATs. Companies engage in differential treatment of user data and accord different protections for the same in their privacy policies. This difference can often be a result of the technological means of collecting data, users' expectation around privacy of their data and very importantly the nature of data. For example, an IP address that is stored in a record of a provider showing a successful login is likely considered to be non-content under US law, and free of the disclosure prohibitions that apply to content. If that same IP address was typed by the user into an email and sent, that email would be considered communications content even though the same information in a log is non-content.

An abstract illustration of a circuit board pattern in shades of brown, tan, and green, with various lines, dots, and geometric shapes representing electronic components and traces. The pattern is dense and complex, filling the upper and side portions of the page.

# Data Requests

# Investigation in India

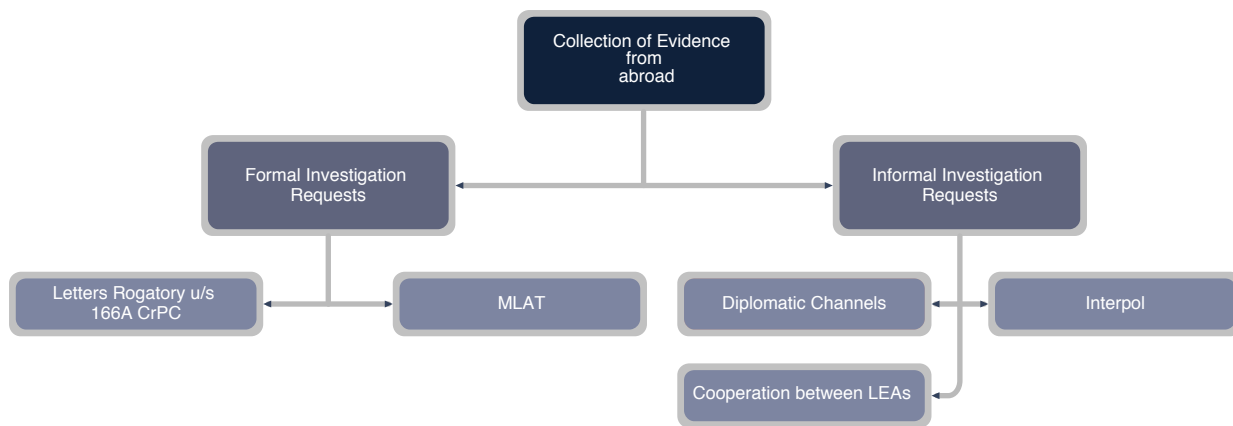
## *Collection of evidence*

An investigating officer (IO) in India when trying to access electronic data to further their investigation has the option of either seizing the hardware belonging to accused – the phone or the hard drive <sup>27</sup>, or accessing the user's data stored by the service provider. An IO in India would resort to a request under S 91 of the CrPC to compel the production of any “document or thing.”<sup>28</sup> Under this section, a police officer only needs to produce a written request to access data when it is considered “necessary or desirable” for an investigation or trial. S.91 under CrPC is used by Indian investigating agencies to obtain non-content data from companies.

## *Admissibility of evidence*

The exclusionary rule is absent under Indian law – irregularity in procedure during collection of records will not disqualify their evidentiary value.<sup>29</sup> There are however standards prescribed to ensure propriety in admissibility of electronic evidence before Indian courts. After the enactment of the IT Act, the Indian Evidence Act, 1872 was amended to insert special provisions for the authentication of electronic evidence. Section 65B(2) of the Evidence Act requires that for an electronic evidence to be admissible, the computer from which the evidence was obtained must have been in regular use and was used for storage within its regular functions. The computer must also have been operating properly during the material part of the investigation. Averments towards the fulfilment of these conditions must be certified by a “senior person” responsible for the operation of the computer system.<sup>30</sup> Only upon fulfilment of these conditions would electronic evidence be admissible in a court.

The process through which an Indian LEA requests non-content is different from the process for retrieval of content data when the communication service provider is headquartered in the US. There is however no difference in the procedure for requesting user data, be it subscriber, traffic or content, when the communication service provider is headquartered in India.



*Fig. 2: Methods through which Indian LEAs can obtain evidence from abroad*

## Direct Requests

### *When LEAs request non-content data from US companies*

The Electronic Communications Privacy Act does not expressly bar US companies from disclosing non-content data in response to requests by foreign LEAs.<sup>31</sup> The largest of the US companies voluntarily respond to requests for non-content data from Indian LEAs within a few days as long as the request is properly made under S. 91 of the Code of Criminal Procedure, 1973 (CrPC).

When responding to requests for user data, companies verify whether the following details have been provided in the S.91 request:

- the request has come from an authorized government email id
- the letter of request has been drafted on an agency letterhead
- it contains the relevant sections under which the crime is being investigated
- it contains the name, rank and identification of the investigating officer
- it contains the case number, if a case has been registered

The authors of this paper learnt through their interviews that police officers in India often do not specify some details or the other as mentioned above. The requests are also in many cases

broad in scope and cover all subscriber information such as the time and date of the creation of the profile, IP addresses used to send messages and content of conversations including text messages and video clips. Police officers also make personal requests for user data, which are not in pursuance of any formal investigation. Companies reject such requests unless due procedure is followed.

Companies, guided by principles of sovereignty and territorial jurisdiction, also take into account a geographical nexus between the activity under investigation and nationality or location of the user. For example, a company may not disclose information to authorities in Japan about the activity of a user if it appears the user is in India; instead they would have the Japanese authorities work with their counterparts in India to secure that information. Similarly, a company may not disclose information about a user who appears to be in Japan to an Indian authority, leaving that to the Indian authorities to work with their Japanese or US counterparts.

### *When LEAs make emergency requests to US companies*

Under the ECPA, companies are permitted to voluntarily disclose customer communications to US governmental entities if there is an emergency involving imminent danger of death or serious physical injury to any person.<sup>32</sup> Companies however also disclose non-content user data to foreign LEAs during emergencies that are life threatening<sup>33</sup> or involve imminent harm to a child<sup>34</sup>. The companies respond to emergency requests, often within hours. They generally operate a round-the-clock helpline where LEAs can request information in cases of emergencies through emails.

LEAs would have to establish the imminence of the threat and seriousness of the harm likely to occur, failing which these requests are declined. At times, the headquarters may even approach their local entities to verify the urgency of the request within the local context. As would be expected, the number of requests made under emergency requests forms a small fraction of the total number of user data requests.<sup>35</sup>

### *When LEAs make data preservation requests*

The ECPA in the US does not mandate compulsory retention of data by communication companies. The SCA however requires companies to preserve data for 90 days upon receiving a request from a government entity in the US.<sup>36</sup> This can be extended for an additional 90 days upon request.<sup>37</sup> Companies also preserve data in response to requests by foreign LEAs, though not required to do so under US law.

Since MLAT requests are time consuming, foreign LEAs also request electronic CSPs to preserve data to ensure that the information is still accessible for investigation purposes. A nodal point for

sending such requests to the G-8 countries has been set up in the Economic Offences division (EO-III) of the Central Bureau of Investigation (CBI) in New Delhi.

Under Indian law, however, data preservation and data retention are treated interchangeably. S.67(c) of the IT Act, titled “Preservation and retention of information by intermediaries,” imposes an obligation on intermediaries in India to retain information in a format, manner and for a duration as prescribed by the Central Government.<sup>38</sup> Data retention, however, is different from preservation. Data preservation follows a specific request by a government agency to store data while the agency goes through a legal process to compel the disclosure of the information. Data retention on the other hand requires companies to store all data for a specific period in the event that the information is needed for an investigation.

Laws calling for data preservation have been viewed to be less detrimental to user privacy than data retention – the former likely to occur only in limited circumstances contingent on a law enforcement agent making a preservation request. The data retention rules under Indian law, however, have not been framed even though a committee was established by the Ministry of Electronics & Information Technology (MeitY) in 2016 to decide the format and time period for the retention of data.<sup>39</sup>

## Formal Requests

Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory (letters of request/LR) are two tools through which law enforcement agencies can seek assistance from foreign law enforcement agencies and courts during criminal investigations.

State police agencies and the CBI apply for a Letters Rogatory when requesting user data located abroad for criminal investigations. The National Investigation Agency (NIA), on the other hand, that deals with terror and national security-related investigations uses MLATs to procure evidence located abroad. Interviews with these agencies revealed that this difference is a result of varying modus operandi of these organisations and the nature of crimes they investigate.

### *MLATs v. Letters Rogatory*

S.105 of the Code of Criminal Procedure (CrPC) empowers the Indian government to enter into reciprocal arrangements with foreign governments to provide assistance for service of summons, warrants and judicial processes abroad.<sup>40</sup> To date, the Indian government has entered into MLATs with 39 countries.<sup>41</sup> MLATs are diplomatic, mostly bilateral agreements entered into between states to exchange evidence and to serve summons during criminal investigations and prosecutions. Letters Rogatory on the other hand are issued by courts and are traditionally considered to have a broader reach as they can be enforced in the absence of a treaty, during criminal, civil and administrative proceedings and are available to private parties<sup>42</sup>

Requests for user data that originate from an Indian investigative agency, either through MLATs or LRs are routed through the central authorities of the requesting and requested states. The central authorities designated for this purpose are Ministry of Home Affairs (MHA) in India and the Office of International Affairs (OIA) under the Department of Justice in U.S.<sup>43</sup> With a view to streamline evidence gathering, the MHA issued guidelines for LEAs on serving summons/notices/judicial processes on persons residing abroad through MLATs and LRs. The only distinction being that LRs<sup>44</sup> need to be issued by a court while MLAT requests can be made directly by LEAs. The systemic problems faced by letters rogatory and MLATs, however are the same since they involve the same agencies and diplomatic channels. In practice, Letters Rogatory are infrequently issued and have been used as a tool to produce summons or obtain evidence from abroad generally in sensational cases.<sup>45</sup>

### *India-US MLAT*

The India-US MLAT was signed under the shadow of growing transnational terrorism. The US was still reeling from the devastation of 9/11 when nearly a month after the attacks, on October 17, 2001 then US Secretary of State, Colin Powell and the Indian Minister of Home Affairs, L. K. Advani signed the MLAT. Increased cooperation between the two states on counter-terrorism was emphasised in no uncertain terms by Powell during his visit.<sup>46</sup> This was also the period when the two countries formalized their intelligence sharing mechanisms and resolved to cooperate on matters of cyber-terrorism and information security.<sup>47</sup>

The treaty governs the sharing of user data between the respective LEAs. A request under the India-US MLAT is made when an Indian LEA seeks information held by a US company and is particularly useful if the LEA cannot get the information directly. Even where there is a possibility of direct disclosure, LEAs may want to use MLAT for purposes of evidence admissibility. Typically this means the content of communications, where the US company is prohibited by US law from disclosing information to foreign law enforcement agencies. The MLAT allows Indian agencies to obtain data stored by US companies regardless of nationality or location of the user. MLAT requests for electronic evidence are most often made to retrieve content data or 'data at rest' that is stored by the company. Requests for data at rest refer to requests for historical information associated with an account that is stored on the company's servers.

The MLAT imposes an obligation on the two countries to offer the widest measure of assistance in the investigation and prosecution of terrorism, narco-trafficking, economic offences and organized crime. The MLAT does not have a dual criminality requirement, instead requiring the subject of investigation to be a crime only in the requesting country.<sup>48</sup> However, the law of the requested state is applicable in so far as the execution of the request is concerned.<sup>49</sup> Courts in the requested state are expected to follow their domestic law while executing requests under an MLAT and can deny the requests only if it is specifically prohibited under their law.<sup>50</sup> This view

has been reiterated in opinions of American courts.

The US Court of Appeals for the Ninth Circuit in 2011 considered the interpretation of the 'execution clause' of the MLAT between US and Russia.<sup>51</sup> The treaty provided that requests would be "executed in accordance with the laws of the Requested Party." The court concluded that the execution of the requests was limited to the procedural mechanism and should not be subject to the substantive limitations under the laws of the requested state.

The scope of assistance envisaged under the India-US MLAT includes execution of searches and seizures<sup>52</sup> and provision of documents, records and items of evidence<sup>53</sup>. Political offences and crimes under military law, however, are excluded from the scope of the MLAT, subject to a few exceptions.<sup>54</sup> These exceptions include widely recognized crimes in international law and multilateral treaties such as aircraft hijacking, hostage taking, and the murder of or willful crime against the head of a state.<sup>55</sup> In other cases, the requested state may also refuse to execute a request made under an MLAT if it would interfere with an ongoing investigation.<sup>56</sup> Under these circumstances, the requested state is obligated to either consult with the requesting state or inform the requesting state the reasons for denial.

The requested state may also compel the requesting state to not use the information provided under the treaty for an investigation other than the one described in the request<sup>57</sup>. This principle has also been reaffirmed by Indian courts. In *Jayalalitha v. State*,<sup>58</sup> the High Court of Madras considered whether the information obtained from the United Kingdom through Letters Rogatory could be used by law enforcement agencies to initiate a separate investigation into and prosecution of allegations of corruption by a government official. The Letters Rogatory in that matter contained an undertaking by the Indian investigating agency which read, "None of the evidence which might be sent by the United Kingdom Authorities to me in this matter will ever be used without their consent, by any authorities in India for any purpose other than the one stated in the Letter of Request." Disallowing the government's request, the court held that while investigations into corruption perpetrated by state officials is of paramount importance, it cannot be made at the cost of violating an undertaking made by Indian law enforcement to a foreign investigating agency. The separate investigation was thus barred from proceeding.



## India side of the process

Indian LEAs, while making MLAT requests are guided by periodic circulars released by the CBI as well as internal standing orders. For instance, Delhi police follows the procedure as laid down by the standing order of the police department, which was circulated, to all officers in 2013. MLAT requests originate from an investigating agency and are sent to the Director of Prosecution in Delhi and to the Criminal Investigation Department and later Home Secretary at the state government level.

The Director of Prosecution in Delhi provides the legal opinion and sends back the request to the investigating agency. The MLAT request along with the legal opinion is sent to Internal Security –II Division at Ministry of Home Affairs. The MHA then forwards the request to the Indian Mission in the US who sends it to the Office of International Affairs (OIA) under the Department of Justice, the central authority in the US (Fig. 3).

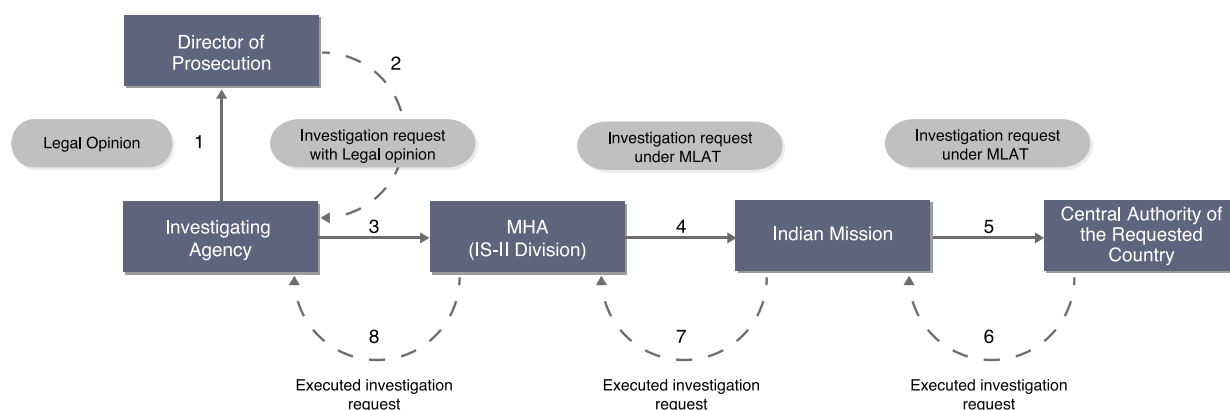


Fig. 3: Indian side of the MLAT request

## US side of the process

In most cases, the OIA examines the request and forwards it to the Attorney General's office who after re-examination places it on a federal court's docket where it is treated equally with all other matters before the court in the US. If the court approves the request, it will issue an order to the company to disclose the information to the US agency. In some other cases, the OIA handles the matters directly. If the court approves the request, it will issue an order to the company to disclose the information to the US agency. If information about US citizens or lawful permanent residents of the US is implicated, then the information undergoes a data minimisation process by the FBI and OIA where incidental data is deleted and the final data is sent to the MHA.

According to the India - US MLAT, a request for user data from the requesting state has to be executed according to the laws of the requested state.<sup>59</sup> Indian LEAs when submitting requests to the MHA will need to ensure that their data requests contain enough information to meet the American 'probable cause' standard. A warrant for stored, content data under Electronic Communications Privacy Act can only be issued when a U.S court finds probable cause to believe that the information sought is evidence of a crime or contraband prior to the disclosure of stored communications content by U.S. communications service providers.<sup>60</sup>

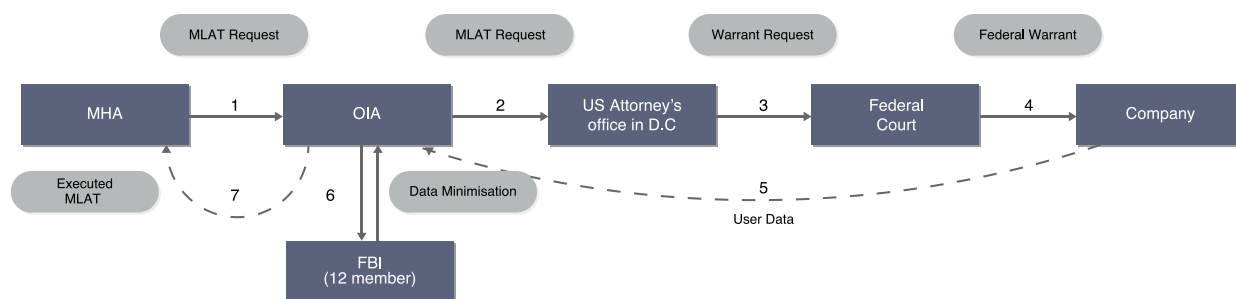
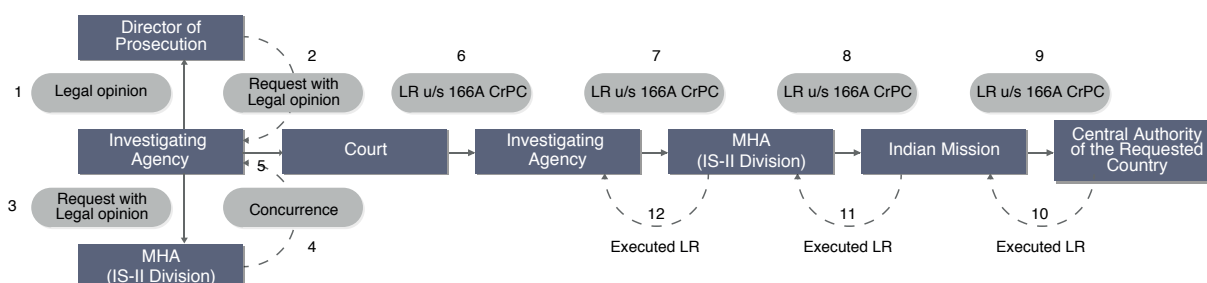


Fig. 4: US side of the MLAT/LR request

## Letters Rogatory



*Fig. 5: Indian side of a letters rogatory request U/S 166A CrPC*

Letters Rogatory can be issued for investigations abroad by any criminal court upon receiving an application by an investigating officer (or any officer superior to an IO) under S. 166-A of the Code of the Criminal Procedure.<sup>61</sup> Letters Rogatory can be issued under a treaty, MOU or on the basis of reciprocity.<sup>62</sup> LRs must be routed through the MHA and in effect the procedure, in India and in the requested state, resembles that of an MLAT request.<sup>63</sup>

Typically the Indian side of the process for a Letters Rogatory takes a total of six months and resembles the process of a request made under MLATs. The investigating officer, before filing an application for an LR in court, will first establish a nexus between the accused and the evidence through a S.166A request under the CrPC.<sup>64</sup> The request under S.166A must provide the legal and factual basis of the case, particulars of the offence and details of the evidence to be produced.<sup>65</sup> The request must also cite the relevant provisions of the laws of the requested state that would criminalise similar conduct in addition to the provisions of the MLAT or MoU that enables the providing of such assistance.<sup>66</sup> In the request the LEA must also undertake that the crime being investigated is not political, military, racial or religious in nature.

The IO submits the request to the Director of Prosecution of the concerned state government for review. The Director of Prosecution, a legal officer under the state, provides a legal opinion on the necessity of issuing an LR. The IO then forwards the S.91 of Cr. P.C request along with the legal opinion to the Internal Security –II Division at the Ministry of Home Affairs (MHA). The MHA evaluates whether the request has been drafted in accordance with the treaty in question and the guidelines issued. The request is then sent back to the IO who presents it before a court of law.

Usually LRs are issued by a Chief Metropolitan Magistrate or a Chief Judicial Magistrate designated for the purpose. While issuing an LR, the court considers the nexus between the accused and

the evidence located overseas. The court assesses the necessity of the evidence requested for the trial to proceed and the convenience in obtaining the evidence. The court generally issues an LR within a month of the request being made by the LEA. The proceedings are generally held in open court. For sensitive investigations, however, the option of in camera hearings may be provided. During a proceeding for an LR, the accused does not enjoy a right to be heard and can only contest evidence at the time of trial.<sup>67</sup> Once a court decides that an LR is necessary for investigation, it is drafted in the language prescribed by the MHA. The US side of the process for an LR request resembles that of an MLAT.



# Key Takeaways

### *Capacity deficit*

A recurring theme in the authors' interviews with law enforcement officials and policy makers was the lack of 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.

### *Process delays*

As a corollary to the capacity deficit in Indian agencies, each step in processing MLAT requests takes an inordinate amount of time. Lack of experienced personnel for handling MLAT requests within the MHA often results in institutional bottlenecks. It also hinders effective response to supplementary requests for information made by a requested country. Similarly, an inadequate number of judges and courts assigned to issue Letters Rogatory causes a backlog of these requests. These delays often result in unsuccessful investigations due to the transient nature of electronic evidence.

### *Indian laws are data agnostic and do not prescribe judicial review*

Unlike the US, Indian laws do not prescribe differential treatment of data depending on whether the data in question is content or non-content. Under S.91 of the CrPC, Indian police officers can issue a notice, without court authorization or review, requesting data from companies, regardless of the kind of data requested. While S.91 allows a court to issue a request for accessing electronic data -- law enforcement agents in India do not approach the court during criminal investigations. Under the IT Act, however, a system for authorization by an executive body is put in place. Section 69 of the Information Technology Act and the rules under the Section allow the Central and State governments to intercept, monitor and decrypt "any information" in pursuance of a criminal investigation. These interception or decryption orders can only be passed by the Secretary in the Ministry of Home Affairs or an officer designated by him. Through the interviews the authors found that police officers usually rely on S.91 of the CrPC and not on the IT Act to access data.

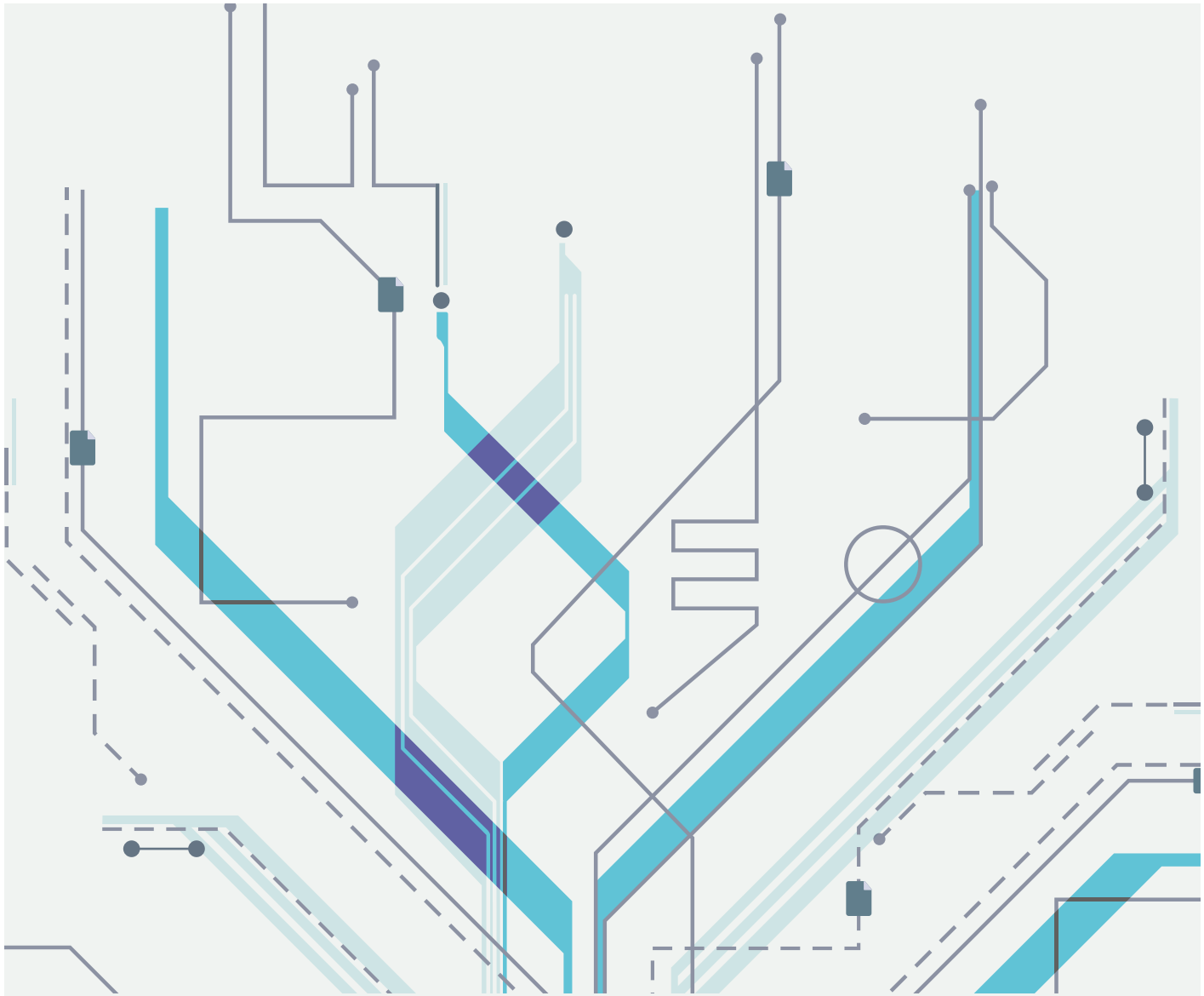
### *Differing roles of regional offices of internet companies*

There is diversity in company practices in dealing with data requests from LEAs. Some companies have clear standards and guidelines for granting law enforcement access to data while others

do not. Where these standards exist, they are a combination of domestic laws of the country the company is incorporated in, international law and the company's internal policies. Some US-based companies rely on their regional arms to comply with non-content data requests by foreign law enforcement agencies whereas others comply with both content and non-content data requests solely through their headquarters in the US.

### *Inclination to supplement MLATs*

MLATs, despite being the most preferred route for formal data sharing between nations, are fraught with formidable institutional problems. In the short term, law enforcement agencies and internet companies are interested in taking remedial steps to make their respective processes more agile and transparent. In the long term, however, policymakers in India are considering supplementing the MLAT mechanism with a direct data sharing agreement that would significantly reduce the time required for conducting investigations. Stakeholders acknowledged that such an agreement however, must rest on a framework of adequate respect for human rights, transparency and oversight.



# Short Term Reforms





## For Companies

### A. Increase transparency in reporting of data requests made under India-US MLAT

US companies comply with content data requests on receiving a warrant under the ECPA issued by a US court. Some sources claim that warrants under MLAT requests do not specify the country of origin of the request. Through the authors' interviews with the US law enforcement agencies, it was reiterated that companies are aware of ECPA search warrants processed as a result of MLAT requests and the country requesting data. This, however, is not true in all cases. Some warrants may specify that the information is being sought through MLATs and identify the country requesting information. Other warrants may not specify the country requesting the information.

Twitter's US transparency report reveals the total number of MLAT requests and countries that made these requests in a year but does not reveal the number of MLATs made by each country.<sup>69</sup> Moreover, Yahoo!'s transparency report for India also reveals the specific number of content data requests made. However, Yahoo! does not make the distinction between content data requests made under MLATs and Emergency Disclosure Requests. These numbers would then indicate the number of requests made under the India-US MLAT where the warrant specified the country of origin. It is recommended that all companies quantify the number of data requests made under MLATs wherever available, the number of requests made under EDRs and number of requests where some information was disclosed.

## For Law enforcement

### B. Specifying kind of data in user data requests

While drafting their requests for data, Indian law enforcement agencies often fail to specify the exact nature of the data that they are seeking. This results from an insufficient technical understanding of what data is available to them and how to request for that data. In some instances, they also send data requests from non-official email IDs. These requests are declined by the OIA and sent back for supplementary information. It was indicated during the interviews that each state has a nodal officer in charge of processing the MLAT request on behalf of the investigating officer and forwarding it to the MHA. These nodal officers are usually police officers belonging to the rank of an Inspector General or Deputy Inspector General. These nodal agents should be equipped with the list of major services/applications offered and their privacy policies .

### C. Institutionalise inter-agency cooperation and build capacity within State and Central Law Enforcement Agencies.

CBI houses the International Police Cooperation Cell (IPCC) which assists investigating officers from CBI and from state police agencies to make requests under LRs. This assistance extends to drafting of the requests, establishing the nexus between the crime being investigated and necessity of the evidence requested and providing templates for future requests. This process, however, is an informal one, often carried out on an ad hoc basis. The cooperation between police agencies and the IPCC needs to be institutionalised so that nodal officers in each state can rely on their expertise. In the long run, each state must establish its own IPCC that can provide legal and practical assistance in drafting requests.

## For Policymakers

### D. Introducing Time Limits for the Indian side of the Process

For the central authority in India to issue an MLAT request, it has to be approved at various stages by the Director of Prosecution, the Court (if it is a request under S. 166A of CrPC) and the MHA. The entire process can take anywhere between 3-6 months. This causes an inordinate delay in the issuance of the data request. It is recommended that strict time limits for review should be introduced for each step of the MLAT process. The MHA has issued guidelines for procedure and review of MLAT requests. Additionally the CBI has issued circulars to guide state police agencies and some state police agencies have issued standing orders to streamline the MLAT requesting process. These documents should incorporate time limits for assessment and review of MLAT requests at each stage. For example, it could be specified that the Director of Prosecution provide his legal opinion on an MLAT within 15 days.

### E. Build Capacity Within MHA

The MHA in its review examines whether the facts and relevant provisions of law have been adequately laid out, along with the required documentation. Complemented with the legal opinion of the Director of Prosecution, it also examines the need to conduct investigation abroad. However, there have been instances where even incorrectly drafted requests have been forwarded by MHA to the OIA. These requests are declined. The MHA should establish a dedicated team of legal officers trained in international criminal law and law enforcement agents on deputation. The legal officers would be able to vet outgoing MLAT requests and examine them against probable cause standards. The law enforcement agents would be able to identify the data required based on the kind of evidence necessary for any particular investigation.

## F. Streamlining process for obtaining supplementary information

In cases where the request is declined and supplementary information is sought, the request for supplementary information is not sent directly to the investigating agency. Instead, it is routed through the same agencies that forwarded it. This is a time consuming process. It is recommended that the request for supplementary information should be sent directly to the IO via email with a copy to the Indian central authority. This will reduce bottlenecks in the process while ensuring that the central authority is apprised of the additional requests. It is also recommended that a specific time limit be prescribed for responding to supplementary requests failing which the original MLAT request will lapse. This can ensure that the IO deals with supplementary requests in an expedited manner and that the number of pending MLAT requests in the requested agency's docket is reduced.

## G. Digitising the Transmission of and Monitoring of MLAT requests

Through the interviews, the authors learnt that law enforcement agencies seldom have the opportunity to track their requests once they are made. This leads to multiple requests being made by the LEAs for the same data, further delaying investigations and prosecution. The central authorities in each country should institutionalise a tracking and monitoring mechanism through which the requesting law enforcement agencies can keep track of their requests and plan an effective timeline for investigations. The process of filing MLATs should also be gradually migrated to an electronic interface that allows for faster transmission of requests while keeping all the relevant agencies in the loop. It can also reduce the costs of transmitting large volume of documents that accompany MLAT requests today. Digitising the process will compel LEAs to draft more concise and self-contained requests and rely less on reams of annexures to establish their need for data. Additionally the government must increase transparency around requests made under MLATs and should make the numbers public such as the number of requests for content data sent to the US.



# Long Term Reforms

## Direct Data Sharing as an Alternative to MLAT

Recognising the difficulty of obtaining timely information under the MLAT process, the United States and the United Kingdom are negotiating a bilateral data-sharing agreement (hereinafter US-UK Agreement) that would allow the UK's law enforcement agencies to request content data directly from U.S companies and vice versa. Currently, the Electronic Communications Privacy Act restricts providers of electronic communications from disclosing communications content data to foreign governments.<sup>70</sup> The US Department of Justice has proposed amendments to the ECPA that would allow US companies to intercept or disclose the content of communications in response to direct requests by foreign governments. These amendments<sup>71</sup> are intended to establish a framework and standards that can be used to reach similar agreements with countries that protect privacy and promote civil liberties.<sup>72</sup> Agreements with such countries would be subject to a determination by the Attorney General (in concurrence with the Secretary of State) that the country meets adequate standards of human rights protections.

The stated objective of the amendments is to enable allies of the US to “combat serious crime, including terrorism”<sup>73</sup> in their territories by accessing data stored by US companies. The investigating agencies in these countries would however, be barred from requesting data relating to US persons or persons residing in the US.<sup>74</sup> In fact, the proposed agreement requires countries to adopt mechanisms to minimize the acquisition, retention and dissemination of information relating to US persons obtained incidentally.<sup>75</sup>

The amendments lay out the basic conditions that a country would need to meet to qualify for a data sharing agreement.<sup>76</sup> It requires the Attorney General to assess whether the country in question offers substantive and procedural protections for privacy and adequately implements these protections. It indicates that accession to the Convention on Cybercrime (hereinafter Budapest Convention) or compliance with the standards prescribed therein is demonstration of having adequate laws on cybercrime and electronic evidence.<sup>77</sup> The amendments prescribe further details for this assessment such as a clear legal mandate for the authorities entitled to seek data and a review mechanism for requests for data. It seeks to ensure that the country seeking the data sharing agreement also has adequate data protection provisions that specify a time limit for storage of data and exhaustion of other means by which the same information could be obtained<sup>78</sup>.

The Agreement once it comes into effect would allow US companies to disclose the content of communications directly to agencies in countries that have such an agreement in place, thus eliminating the need for MLATs in most circumstances. This would extend to requests for content of electronic communications as well as real-time tap and trace of communications.

The US-UK data sharing agreement is a product of years of negotiations and bilateral relations, both diplomatic as well as legal.<sup>79</sup> A similar arrangement between India and the US will require the countries to find an effective middle ground in regulations governing access, retention and dissemination of data. This agreement, however, will only come to fruition if Indian law meets the three basic elements of the Attorney General's assessment. These elements are "factors" that the US AG must consider before agreeing to enter into a data sharing agreement. First, that Indian law affords robust substantive as well as procedural protections for privacy; Second, that India has appropriate procedures to minimise the acquisition, retention and dissemination of information about US citizens; Third, that data requests are made under Indian law, are subjected to immediate review and not used for bulk data collection.

India objectively meets several factors laid out under the amendments and can qualify as a like-minded country in its commitment to an open and free internet. India has affirmed its support for an open internet and global free flow of information not only in international fora like ICANN<sup>80</sup> but also in its bilateral relations with the US. The Framework for U.S Cyber Relationship signed by both states in 2016 affirms a commitment to an open, interoperable, secure and resilient cyberspace.<sup>81</sup> It also affirms a commitment to promote the free flow of information over the internet. There are however, many aspects of India's legal and regulatory regime that would fall short of the qualifications laid out in the amendments.

The proposed ECPA amendment requires requests from the foreign government to meet certain standards in access, retention and dissemination of data and imposes higher standards for real-time interception requests. India's data protection framework is located in rules issued under the IT (Amendment), Act, 2008 – Sensitive Personal Data Rules, 2011 and the Interception Rules, 2009. In the absence of a single data protection law, designated regulatory authority, enforceable rules against public agencies and a fundamental right to privacy -- privacy is still at a nascent stage.

Indian laws do not impose requirements addressing targeting, reasonable justification and judicial oversight. When it comes to access to data, Indian laws are data agnostic with no distinction drawn between content and non-content data. An Indian law enforcement agent can obtain data by issuing a notice to the CSP, under S.91 of the CrPC, without court authorization or review, India lacks any form of judicial oversight on collection of data not only under S.91 but also under Section 69 of the IT Act for interception of communications. The IT Act provides some protections for real-time collection of data by providing temporal limits on interception of communications and retention of collected data. At the same time, there is little transparency on the number of interception orders passed and the frequency of Review Committee meetings.

The table below provides a comparison of standards required under the proposed ECPA amendment for a foreign government to meet to enable US to enter into bilateral data sharing agreement and current Indian laws. India's laws stand up to scrutiny on some of the below

standards required and fall short in some others. With the government is likely to propose a new data protection regime by the end of the year and a nine judge bench at the Supreme Court currently deciding whether Indian citizens enjoy a fundamental right to privacy -- data protection regulations in India can be transformed soon. In the aspects where India is lacking adequacy in data protection laws, policymakers should strive to introduce amendments and ensure adequate safeguards if they hope to see a data sharing agreement come to fruition.

Proposed ECPA Amendment	Indian Law
Specificity about the target, device or account	<p>Rule 9 of the Interception Rules provides for the collection of information relating to a person or class of persons or a computer resource or a set of premises. <i>This provision does not ensure the collection of information only of a specific target. It allows for all persons over a computer network engaging in communication about a monitored subject matter to be brought under the ambit of surveillance.</i></p> <p>In practice, requests for collection of information U/S 91 of the CrPC contain details of a specific account (or phone number associated with the account) for collection of information. <i>There is nothing in law requiring the specific identification of a target for collection of information.</i></p>
Orders must be for prevention, detection, investigation, prosecution of serious crime, including terrorism	<p>U/S 69 of the IT Act, orders for collection of information can be issued for protecting the sovereignty and integrity of India, security of the State, maintenance of public order, preventing incitement of a crime or investigation of any offence. <i>This provision allows for interception for investigation of any crime, not just a serious crime. Indian law does not define ‘serious crimes.’</i></p> <p>S. 91 of CrPC authorises a court or an investigating agency to collect any document that is “necessary or desirable” for the purpose of an investigation.</p>
Orders to be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation	<p>U/S. 69 of the IT Act, the Competent Authority issuing the order for interception must satisfy himself that the interception is necessary or expedient in the interest of national security or public safety. <i>There are, however, no objective criteria prescribed in the Act on the basis of which an authority is meant to arrive at these conclusions. He must, in that case, necessarily arrive at these findings on a discretionary assessment of the facts and circumstances.</i></p> <p>U/S.166A of CrPC, an investigating officer must apply for a letter of request from a competent court to obtain evidence from abroad. The court examines the nexus between the location of the evidence and the crime being investigated. The court also examines the necessity of the evidence for the investigation of the offence before issuing the order.</p> <p><i>It is unclear whether LEAs in India will need to approach the court under S.166A to obtain data under a bilateral agreement. In the absence of this requirement, LEAs will rely on S.91 of the CrPC to request data. S.91 does not impose any requirements of reasonable justification. Such requests are not authorized or reviewed by a judicial or an executive body.</i></p>



<p>Orders issued by the foreign government must be subject to review or oversight by a court, judge, magistrate, or other independent authority</p>	<p>Orders for collection of information U/S. 69 of the IT Act are issued by an executive authority who is a Secretary in the Ministry of Home Affairs or a senior official designated by him. These order are subject to review by a 3-member body established under Rule 419A of the Indian Telegraph Rules. The Committee examines whether orders for interception have been passed in accordance with the provisions of S.69 of the IT Act. The review committee is mandated to meet at least once in two months to conduct a review of the orders passed.</p> <p><i>However, an application under the Right to Information Act to the Ministry of Home Affairs has revealed that on an average 7500 to 9000 orders for interception are issued every month by the Central Government alone. Therefore, if the Review Committee meets once every two months as it is statutorily mandated to do, then it would have to consider and dispose of between 15000 to 18000 orders of interception at every meeting. If on the other hand the Review Committee were to meet every day of the month it would have to dispose of between 290 to 345 orders.</i></p>
<p>Orders for interception of data to be for a fixed, limited duration and exhaustion of less intrusive means</p>	<p>Under Rule 11 of the Interception Rules, any direction for interception will only remain in force for a period not exceeding sixty days from the date of its issue. The interception orders can be renewed for a period not exceeding a total period of 180 days.</p> <p>Rule 8 of the Interception Rules impose an obligation on the authority issuing the order to consider the possibility of acquiring the information by other means and issue the order only when it is not possible to acquire the information by any other reasonable means</p>
<p>Prompt review of material collected and secure storage of unreviewed information</p>	<p><i>The IT Act or the rules thereunder do not contain any provision to ensure a prompt review of the information collected.</i></p>
<p>Segregation, deletion and non-dissemination of information not necessary for investigations</p>	<p>Rule 23 of the Interception Rules provides for destruction of records of interception, monitoring and decryption of information. It states that every record relating to an interception order and the information so collected will be destroyed every six months unless it is established that the information is required for an ongoing investigation, criminal complaint or legal proceeding. After the interception has concluded, the intermediary or person in charge of the computer resources is required to destroy all records pertaining to the interception within two months.</p> <p>Rule 25(1) and (2) of the Interception Rules impose an obligation on intermediaries and government agencies to not use or disclose the content of any information obtained through interception. The information collected can only be disclosed by government agencies with other security agencies for investigations or during judicial proceeding before a competent court.</p>



# Conclusion

The cooperation between India and the United States on issues of cyber security has significantly advanced over the past decade. The signing of the Framework Agreement on Cyber Issues in 2016 represents an acknowledgement between both countries that continued cooperation in cyberspace is essential for their economies. Even at 26% internet penetration, India's user base is already a critical market for many US companies. As the number of internet users in India increases, the importance of earning their trust will only rise. Consequently, this will also make Indian law enforcement more dependent on these companies for lawful investigations. As a participant at the India-US Track 1.5 Dialogue on Cyber Issues pointed out, law enforcement access to data remains the single most important concern in the India-US cyber relationship.

In the conversations that the authors had with various law enforcement agents and internet companies, user privacy emerged as a central consideration for both stakeholders. Neither found access to data while compromising privacy a desirable proposition. However, Indian legal standards for accessing data suffer from a lack of oversight. These standards that derive from legacy legislations do not readily apply to electronic data and the ubiquity of internet services. Access to data under Indian laws does not require judicial authorization, which often conflicts with the US probable cause standard. The conflict between Indian and US laws be it with respect to how LEAs access data or how companies use data may never be fully compatible. However, this conflict should not undermine a legitimate need for data for investigations. Efforts need to be made from both sides to arrive at a middle ground.




Indian data protection laws need guidance through clear and detailed regulations that specify limits on access, storage and handling of data. American companies that are subject to US laws selectively extend the privacy safeguards guaranteed under US laws to their international users. Reforms to the ECPA should help clarify the application of the provisions in the Act to non-US users, law enforcement agents and governments.

While policymakers consider alternatives like data sharing they must not lose sight of the fact that MLATs will not be rendered obsolete. MLATs will still be required for obtaining data from jurisdictions other than the US. The India-US MLAT will remain central to obtaining data from the US about non-Indian citizens and US citizens. It is likely that even under a data sharing agreement a form of governmental oversight will be deemed necessary in both states. Given the fact that MLATs will continue to operate in tandem with a data sharing agreement, policymakers must also focus their attention towards short term reforms such as capacity building, digitisation and increased cooperation between Indian LEAs and US companies.

Cooperation on data sharing represents an attempt by two sovereign nations to create artificial limitations on the ownership of data to further investigations. This process cannot move forward without the necessary political will on both sides. The impending US-UK data sharing agreement is

a product of this political will. Conversations between India and the US are grounded in a different political context. Indian policymakers are open to considering alternatives to the inefficient MLAT process. However they must be willing to reimagine and amend domestic laws to make privacy of individuals a central concern. They must also be willing to address the capacity deficit within Indian institutions. No alternative to an MLAT would be successful if the Indian standards for accessing user data remain unpredictable. Similarly no reforms even if adopted would be effective unless institutional bottlenecks are removed. As an interviewee noted, any MLAT alternative will not be worth the paper it is written on unless both countries enable a productive dialogue between their law enforcement agencies and the private sector.

## Appendix I: Data as classified by major communication providers<sup>i</sup>

	<p>Non-content information – includes basic subscriber information, e.g., email address and phone number associated with the account and transactional information, e.g., the to/from of a Direct Message.</p> <p>Content information includes the contents of communications associated with an account, e.g, Tweet content, DM content, Vines, Periscope broadcasts.<sup>ii</sup></p>
	<p>Broadly Facebook collects the following information:<sup>iii</sup></p> <p>Things users do and information users provide – includes information provided during sign-up, information in or about the content you provide, e.g. location of a photo and information about how users use FB’s services, e.g. content viewed.</p> <p>Things others do and information they provide – Includes information that other users provide when they use FB Services, e.g, when a user shares a photo tagging another, sends a message or imports contact information.</p> <p>Information about payments – Includes payment information, and other account and authentication information, as well as billing, shipping and contact details.</p> <p>Device information – Includes attributes such as device settings and device identifiers, device locations, connection information</p> <p>Information from websites and apps that use our Services – FB collects information when users visit or use third party website apps that use their services such as the Like or Log In buttons. FB also collects information the developer or publisher of the app or website provides to the user/FB.</p> <p>Information from third-party partners— Information about users and their activities on and off Facebook from third-party partners, e.g, information from an advertiser about user experiences or interactions with them.</p> <p>Facebook companies – FB receives information about users from companies that are owned or operated by Facebook, in accordance with their terms and policies.</p>
	<p>Google in its privacy policy<sup>iv</sup> elaborates on the different kind of data it collects, along with examples, which includes:</p> <ul style="list-style-type: none"> <li>- Personal information such as name, email address, billing information etc.</li> <li>- Device, log, location information</li> </ul> <p>In the Google Transparency report<sup>v</sup>, Google gives examples of data that falls in the content and non-content categories and the types of legal process under US law required to compel disclosure.</p>



NCD: Non-content data such as basic subscriber information (including the information captured at the time of registration, such as an alternate e-mail address, name, location, and IP address), login details, billing information and other transactional information (e.g., "to," "from," and "date" fields from email headers).

Content: Data that our users create, communicate, and store on or through our services. This could include words in a communication, e.g., Mail or Messenger, photos on Flickr, files uploaded, Yahoo Address Book entries, Yahoo Calendar event details etc.<sup>vi</sup>



Non-content data include basic subscriber information, such as email address, name, state, country, ZIP code, and IP address at time of registration. Other non-content data may include IP connection history, an Xbox gamertag, and credit card or other billing information.

Content is what our customers create, communicate, and store on or through our services, such as the words in an email exchanged between friends or business colleagues or the photographs and documents stored on OneDrive (formerly called SkyDrive) or other cloud offerings such as Office 365 and Azure.<sup>vii</sup>



Device Registration - Basic registration or customer information, including, name, address, email address, and telephone number is provided to Apple by customers when registering.

Customer Service Records - Contacts that customers have had with Apple customer service regarding a device or service may be obtained from Apple.

Apple Online Store Purchases - Apple maintains information regarding Apple Online Store purchases, which may include name of the purchaser, shipping address, telephone number, email address, product(s) purchased, purchase amount, and IP address of the purchase







iCloud - The following information may be available from iCloud: i. Subscriber information, ii. Mail Logs, iii. Email Content and Other iCloud Content. My Photo Stream, iCloud, Photo Library, iCloud Drive, Contacts, Calendars, Bookmarks, Safari Browsing History, iOS Device Backups







Services such as Facetime, iMessage are end-to-end encrypted.

Other Available Device Information: MAC Address, UDID, CCTV Data of Apple Retail stores, iOS Device Activation, ICCID numbers, and other device identifiers. My Apple ID and iForgot logs may include information regarding password reset actions.<sup>viii</sup>







## Appendix II:

### Reporting Practices of major communication providers for India

	 <sup>i</sup>	 <sup>ii</sup>	 <sup>iii</sup>	 <sup>iv</sup>	 <sup>v</sup>	 <sup>vi</sup>
Does the company have a clear policy on notifying foreign users?	No	No	No	No	No	Yes, Apple addresses notifications of foreign users separately.
Does the TR identify the number of accounts specified in government requests?	Yes	Yes	Yes	Yes	Yes	For devices, Apple's Transparency report mentions the number of devices specified in the requests.
Does the company reveal the number of Emergency Disclosure Requests (EDR) made?	Yes, Twitter reveals the number of EDRs.	Yes, Facebook's TR reveals the number of EDRs made.	Yes, Google's TR provides for the number of ED requests made.	No, Yahoo does not reveal the number of EDRs as per country	Yes, Microsoft reveals the number of EDRs received and provides percentages of when content, non-content or no data is disclosed.	Yes
Does the TR break down the number of requests for different services?	No, Twitter includes requests from Periscope and Vine within total requests. However individual breakups by services are not indicated.	No, Facebook does not provide a breakup of government requests according to different services. The total number of government requests in transparency reports include requests made to Facebook Messenger, WhatsApp and Instagram.	No, Google does not provide a breakdown of requests for each service, eg. YouTube, Web Search	No, Yahoo's reports do not include data requests from Tumblr	No, Microsoft does not divide requests as per services.	Apple's Transparency reports break down requests according to devices, financial identifiers and accounts.

						
Does the company have a separate guide for foreign law enforcement agencies?	No	No	Google on its 'Legal process' page answers commonly asked questions about how Google responds to data requests. The legal process page addresses data requests from outside U.S separately.	Yahoo in their Law Enforcement Guidelines has a section dedicated to requests from outside US.	No	Yes, Apple has a separate policy titled Legal Process Guidelines for Government and Law Enforcement
How does a company vet the requests?	Twitter looks for the following in data requests: - @username and URL of the account requested -Details about what specific information is required, eg. BSI, provided the same is not available through public API. -A valid email address -Law enforcement letterhead	Facebook evaluates government requests on the basis of: -Legal and factual sufficiency by law in that jurisdiction, -whether it affects users in that jurisdiction -whether response would be consistent with internationally recognized standards.	Google evaluates government requests on the basis of: -if those requests are consistent with international norms, U.S law, Google policies and law of the requesting country	Legal processes must comply with applicable substantive and procedural requirements for the issuance of that type of process. In addition to requiring that all requests for user data comply with ECPA and other applicable laws, we also require that: -The legal process must contain appropriate identifiers -All process must be submitted in writing - All process must be on official letterhead and other authorization information	Microsoft adheres to the same principles for all requests from government agencies for user data requiring governmental entities to follow the applicable laws, rules and procedures for requesting customer data. Requests must be targeted and specify identifiers.	Apple requires government and private entities to follow applicable laws and statutes when requesting customer information and data. Our legal team reviews requests received to ensure that the requests have a valid legal basis. Requests must not be unclear, inappropriate or over-broad.



						
Does the TR identify the number of requests received through MLATs/ LRs?	Yes, the US transparency reports reveal the percentage of court orders received through MLATs in total. Twitter does not reveal if information was produced in response to these MLAT requests.	No	No	Yahoo in its India TR reveals the number of content data requests made. However, Yahoo! does not make the distinction between content data requests made under MLATs and EDRs.	No	No
Does the company explain how Indian LEAs access content and non-content data?	No	No	No	No	No	No
What is the company's policy on preserving data?	Twitter can preserve temporary snapshots of relevant account records for 90 days in response to account preservation requests from LEAs. Twitter also provides for 'preservation extension' requests, where account information can be saved for an additional 90 days. Twitter's TR reveals the number of account preservation requests made along with accounts specified.	Facebook preserves account records for 90 days once they receive official preservation requests. Preservation requests can be sent in through the Law Enforcement Online Request system. Facebook's TR reveals the number of data preservation requests made by India along with the accounts specified in the requests.	Google's India Transparency Report mentions the number of data preservation requests made by Indian agencies.	Yahoo preserves user data, to the extent it is available, for 90 days upon receipt of a valid preservation request from a government agency issued in accordance with applicable law. Yahoo's India TR does not reveal the number of data preservation requests.	No, Microsoft's India TR does not reveal the number of data preservation requests made.	When a preservation request has been received, Apple Inc. will preserve a one-time data pull of the requested existing user data available at the time of the request for 90 days. After this 90 day period, the preservation will be automatically removed from the storage server. However, this period can be extended one additional 90-day period upon a renewed request

# Endnotes

1. Jeekeshen Chinnappen, "Understanding Data Localization Laws," *BigBang ERP*, August 17, 2016, accessed August 8, 2017, <https://bigbangerp.com/data-localization-laws/>.
2. Brad Haynes, "Facebook executive jailed in Brazil as court seeks WhatsApp data," *Reuters*, March 1, 2016, accessed August 8, 2017, <http://www.reuters.com/article/us-facebook-brazil-idUSKCN0W34WF>.
3. Steven De Schrijver and Thomas Daenens, "The Yahoo! Case: The End of International Legal Assistance In Criminal Matters" *WhosWhoLegal*, September 2013, accessed August 8, 2017, <http://whoswholegal.com/news/features/article/30840/the-yahoo-case-end-international-legal-assistance-criminal-matters>.
4. The Wire Staff, "Government Appoints Committee To Study Data Protection Framework for India," *The Wire*, August 1, 2017, accessed August 8, 2017, <https://thewire.in/163705/committee-data-protection-framework/>.
5. "Facebook Users by Country | Statistic", *Statista*, April 2017, accessed August 7, 2017, <https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/>.
6. Manish Singh, "Guess WhatsApp's biggest market? India," *Mashable*, February 24, 2017, accessed August 7, 2017, [http://mashable.com/2017/02/24/whatsapp-india-200-million-active-users/#k47\\_JHiiksqH](http://mashable.com/2017/02/24/whatsapp-india-200-million-active-users/#k47_JHiiksqH).
7. Subhayan Chakraborty "India fastest growing market for us: Uber", *Business Standard*, August 30, 2016, accessed August 8, 2017, [http://www.business-standard.com/article/companies/india-fastest-growing-market-for-us-uber-116082900959\\_1.html](http://www.business-standard.com/article/companies/india-fastest-growing-market-for-us-uber-116082900959_1.html).
8. Simone Foxman, "The US is home to one third of the world's data—here's who's storing it," *Quartz*, July 17, 2013 accessed August 8, 2017, <https://qz.com/104868/the-us-is-home-to-one-third-of-the-worlds-data-heres-whos-storing-it/>.
9. Samantha Besson, "Sovereignty in Conflict," *European Integration online Papers* Vol. 8 (2004) N° 15, accessed August 8, 2017, <http://eiop.or.at/eiop/pdf/2004-015.pdf>.
10. Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime," *McAfee*, June 2014, accessed August 8, 2017, <https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf>.
11. Ethan A. Nadelmann, "Negotiations in criminal law assistance", *The American Journal of Comparative Law*, Volume 33, Issue 3, 1 July 1985, Pages 467–504, Accessed August 8, 2017, <https://doi.org/10.2307/840237>.
12. Office of the Press Secretary, "FACT SHEET: Framework for the U.S.-India Cyber Relationship," *The White House*, June 7, 2016, accessed August 8, 2017, <https://obamawhitehouse.archives.gov/the-press-office/2016/06/07/fact-sheet-framework-us-india-cyber-relationship>.
13. 18 U.S. Code § 2510(8), Definitions.
14. Refer Appendix I where user data as defined by different companies have been compared. Some company policies distinguish types of data depending on the services used.
15. "What is metadata?", *Privacy International*, accessed August 8, 2017, <https://www.privacyinternational.org/node/53>.
16. Liz Woolery, Ryan Budish, and Kevin Bankston, "The Transparency Reporting Toolkit: Best Practices for Reporting on U.S. Government Requests for User Information," *Berkman Klein Center for Internet and Society*, March 31, 2016, accessed August 8, 2017, [https://cyber.harvard.edu/publications/2016/transparency\\_memos](https://cyber.harvard.edu/publications/2016/transparency_memos).
17. James A. Lewis, Denise E. Zheng, William A. Carter, "The Effect of Encryption on Lawful Access to Communications and Data," *Center for Strategic and International Studies*, February 8, 2017, accessed August 8, 2017, <https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data>.
18. Council of Europe, "Explanatory Report to the Convention on Cybercrime," *Council of Europe*, European Treaty Series - No 185, ¶227, accessed August 8, 2017, <https://rm.coe.int/16800cce5b>. Interestingly the delegates noted that metadata is less revealing than content data and therefore has lesser privacy protections. This distinction may no longer hold true as increasing amounts of metadata about communications are collected and when analyzed en masse, can be revelatory, See also "International Principles on the Application of Human Rights to Communications Surveillance," Necessary And Proportionate, May 2014, accessed August 8, 2017, <https://necessaryandproportionate.org/principles>.
19. Refer Appendix I. Data as defined by major communication companies has been compared.
20. Orin S. Kerr, "The Next Generation Communications Privacy Act," 162 *University of Pennsylvania Law Review* 373 (2014), accessed August 8, 2017, <https://ssrn.com/abstract=2302891>.
21. 18 U.S. Code Chapter 121 - Stored Wire And Electronic Communications and Transactional Records Access, 18 U.S. Code, Chapter 119 - Wire and Electronic Communications Interception And Interception Of Oral Communications and 18 U.S. Code Chapter 206 - Pen Registers and Trap and Trace Devices
22. *Supra* n 16. No warrant, '(d)order', or subpoena will be required.
23. 18 U.S. Code § 2702 (c) - Voluntary disclosure of customer communications or records
24. Greg Nojeim explains how "Although ECPA bars U.S. service providers from voluntarily disclosing metadata to "governmental entities" (18 U.S.C. 2702(c)(6)), the Act defines governmental entity to include only U.S. federal, state and local government agencies (18 U.S.C. 2711(4)). This definition does not include foreign governments. Therefore, U.S. communication service providers are permitted to voluntarily disclose user metadata—be it of a U.S. or non-U.S. person—to other governments": Greg Nojeim, "MLAT Reform Proposal: Protecting Metadata," December 10, 2015, *Lawfare*, accessed August 8, 2017, <https://www.lawfareblog.com/mlat-reform-proposal-protecting-metadata>
25. *U.S. v. Warshak* (631 F.3d 266), *Supra* n.8
26. The U.S Fourth amendment states that "The right of the people to be secure in their persons, houses, papers, and

effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”, For more information on the applicability of Fourth Amendment to seizure of digital data, see Jennifer C. Daskal, “The Un-Territoriality of Data,” 125 Yale Law Journal 326 (2015), accessed August 8, 2017 <http://www.yalelawjournal.org/article/the-un-territoriality-of-data>.

27. S. 93, Code of Criminal Procedure, 1973.
28. S. 91, Code of Criminal Procedure, 1973.
29. State Of Maharashtra v. Natwarlal Damodardas Soni, AIR 1980 SC 593; Radhakrishnan v State of UP, 1963 Supp. 1 S.C.R. 408.
30. Section 65B(4), Indian Evidence Act, 1872.
31. 18 U.S.C. 2702(c)(6), Voluntary disclosure of customer communications or records
32. 18 U.S. Code § 2702(b)(8), Voluntary disclosure of customer communications or records
33. Google Transparency Report - Legal Process, accessed, August 8, 2017 [https://www.google.com/transparencyreport/userdatarequests/legalprocess/#how\\_does\\_google\\_respond](https://www.google.com/transparencyreport/userdatarequests/legalprocess/#how_does_google_respond).
34. Facebook, Information for Law Enforcement Authorities, accessed August 8, 2017 <https://www.facebook.com/safety/groups/law/guidelines/>.
35. Between January and June 2016, the total number of user data requests was 3,438 while the number of requests under emergency disclosure was 14. Google Transparency Report, India, accessed August 8, 2017, <https://www.google.com/transparencyreport/userdatarequests/IN/>.
36. 18 U.S. Code § 2703(f)(1), Required disclosure of customer communications or records.
37. 18 U.S. Code § 2703(f)(2), Required disclosure of customer communications or records.
38. S. 67(C), Information Technology Act, 2000.
39. Surabhi Agarwal, “Tech companies like Gmail, WhatsApp may be asked to store user information,” *The Economic Times*, October 14, 2016, accessed August 8, 2017 [http://economictimes.indiatimes.com/tech/ites/tech-companies-like-gmail-whatsapp-may-be-asked-to-store-user-information/articleshow/54839888.cms?utm\\_source=contentofinterest&utm\\_medium=text&utm\\_campaign=cppst](http://economictimes.indiatimes.com/tech/ites/tech-companies-like-gmail-whatsapp-may-be-asked-to-store-user-information/articleshow/54839888.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst).
40. S. 105, Code of Criminal Procedure, 1973.
41. “MLATs,” Central Bureau of Investigation, accessed August 8, 2017, <http://www.cbi.nic.in/interpol/mlats.php>.
42. Markus Funk, T. “Mutual Legal Assistance Treaties and *Letters Rogatory*: A Guide for Judges,” *Federal Judicial Centre, International Litigation Guide* (2014), accessed August 8, 2017, <https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf>.
43. “Mutual Legal Assistance Treaties,” Ministry of External Affairs, Government of India, accessed August 8, 2017, <http://www.mea.gov.in/mlatcriminal.htm>.
44. Amar Chand (Under Secretary to the Government of India), “Comprehensive guidelines regarding service of summons/ notices/Judicial process on the persons residing abroad,” Circular No. 25016/17/2007, February 11, 2009, accessed August 8, 2017, [http://cbi.nic.in/interpol/mha\\_circ\\_service\\_process.pdf](http://cbi.nic.in/interpol/mha_circ_service_process.pdf).
45. “Sheena Bora murder case: CBI to send *Letters Rogatory* to Singapore, Hong Kong, US,” *Zee News*, April 13, 2016, accessed, August 8, 2017, [http://zeenews.india.com/news/india/sheena-bora-murder-case-cbi-to-send-letters-rogoratory-to-singapore-hong-kong-us\\_1875812.html](http://zeenews.india.com/news/india/sheena-bora-murder-case-cbi-to-send-letters-rogoratory-to-singapore-hong-kong-us_1875812.html). Express News Service, “Louis Berger case: MHA nod to issue Letters Rogatory to US court,” *The Indian Express*, August 31, 2015, accessed August 8, 2017, <http://indianexpress.com/article/india/india-others/louis-berger-case-mha-nod-to-issue-letters-rogoratory-to-us-court/>. PTI, “Mumbai court issues Letter Rogatory to UK in PMLA case against Vijay Mallya,” February 3, 2017, accessed August 8, 2017, <http://economictimes.indiatimes.com/news/politics-and-nation/mumbai-court-issues-letter-rogoratory-to-uk-in-pmla-case-against-vijay-mallya/articleshow/56960850.cms>
46. Sonia Trikha, “Powell treads tightrope, Delhi does not push,” *The Indian Express*, October 17, 2001 accessed August 8, 2017, <http://archive.indianexpress.com/old/ie20011018/top2.html>. Special Correspondent, “India, U.S. sign treaty on legal assistance,” *The Hindu*, October 17, 2017, accessed August 7, 2017 <http://www.thehindu.com/thehindu/2001/10/18/stories/01180005.htm>
47. Bahukutumbi Raman, “Indo-US Counterterrorism Cooperation: Past, Present and Future” in *US-Indian Strategic Cooperation Into the 21st Century: More Than Words*, Ed. Sumit Ganguly et al, Routledge, 2006.
48. Article 1(3), Treaty Between the Government of the Republic of India and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters (India-US MLAT). As a general rule, MLATs with the United States do not have a dual criminality requirement.
49. Article 5(3), India-US MLAT
50. Kimberly Prost, “Breaking Down The Barriers: Inter-National Cooperation In Combating Transnational Crime,” *Organisation of American States*, 1998, accessed August 8, 2017, [https://www.oas.org/juridico/mla/en/can/en\\_can\\_prost.en.htm](https://www.oas.org/juridico/mla/en/can/en_can_prost.en.htm)
51. In re Search of Premises Located at at 840 140th Ave. NE, Bellevue, Wash., 634 F.3d 557 (2011)
52. Article 1(2)(f), India-US MLAT.
53. Article 1(2)(b), India-US MLAT.

54. Article 3(1), India-US MLAT.
55. Article 3(2), India-US MLAT.
56. Article 5(5), India-US MLAT.
57. Article 7(1), India-US MLAT.
58. Jayalalitha v. State, 2002 Cri LJ 3026
59. Article 5(3), India-US MLAT
60. Can be extracted from a combined reading of 18 U.S.C 3512 and 18 U.S.C 2703.
61. S. 166A, Code of Criminal Procedure, 1973.
62. Delhi Police Standing Order No. 427/2013. LC Goyal (Joint Secretary to the Government of India), "Comprehensive Guidelines on Investigations Abroad and Issue of Letters Rogatory," December 31, 2007, accessed, August 8, 2017, <http://cbi.nic.in/interpol/invletterrogatory.php>.
63. S. 166A, Code of Criminal Procedure, 1973. LC Goyal (Joint Secretary to the Government of India), "Comprehensive Guidelines on Investigations Abroad and Issue of Letters Rogatory," December 31, 2007, accessed, August 8, 2017, <http://cbi.nic.in/interpol/invletterrogatory.php>.
64. S 91, Code of Criminal Procedure, 1973.
65. Delhi Police Standing Order No. 427/2013. LC Goyal (Joint Secretary to the Government of India), "Comprehensive Guidelines on Investigations Abroad and Issue of Letters Rogatory," December 31, 2007, accessed, August 8, 2017, <http://cbi.nic.in/interpol/invletterrogatory.php>.
66. Ibid
67. UOI v. Chadha, AIR 1993 SC 1082: 1993 Cri LJ 859
68. Andrew Woods, "Data Beyond Borders: Mutual Legal Assistance In The Internet Age," *Global Network Initiative*, January 2015, accessed August 8, 2017, <https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf>
69. Twitter, Transparency Report for United States, accessed August 8, 2017, <https://transparency.twitter.com/en/countries/us.html>
70. 18 U.S. Code § 2511 - Interception and disclosure of wire, oral, or electronic communications prohibited.
71. Office of Legislative Affairs, "Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism" (Data Sharing Agreement), *US Department of Justice*, July 15, 2016, accessed August 8, 2017, [https://www.aclu.org/sites/default/files/field\\_document/doj\\_legislative\\_proposal.pdf](https://www.aclu.org/sites/default/files/field_document/doj_legislative_proposal.pdf).
72. Peter J. Kazdik, Assistant Attorney General, US Department of Justice, in Letter to Joseph R. Biden, President, United States Senate, July 15, 2016, [https://www.aclu.org/sites/default/files/field\\_document/doj\\_legislative\\_proposal.pdf](https://www.aclu.org/sites/default/files/field_document/doj_legislative_proposal.pdf).
73. Section 2(1), Data Sharing Agreement
74. Section 4(a)(3)(i), Data Sharing Agreement
75. Section 4(a)(2), Data Sharing Agreement
76. Section 4, Data Sharing Agreement.
77. Section 4(a)(1)(i), Data Sharing Agreement.
78. Section 4(a)(3)(ix), Data Sharing Agreement.
79. "Indian Government Declares Support for Multistakeholder Model of Internet Governance at ICANN53," *ICANN*, June 22, 2015, accessed August 8, 2017, <https://www.icann.org/resources/press-material/release-2015-06-22-en>.
80. Ministry of External Affairs, Government of India, "Fact Sheet on the framework for the US-India Cyber Relationship," June 07, 2016, accessed August 8, 2017 <http://mea.gov.in/outgoing-visit-detail.htm?26880/Fact+Sheet+on+the+framework+for+the+USIndia+Cyber+Relationship>.

## Appendix I

- i. This is an indicative list of the types of data as classified by major communication providers in their Transparency Reports, privacy policies and other relevant policies on their websites.
- ii. Twitter, Information Requests, accessed August 8, <https://transparency.twitter.com/en/information-requests.html>
- iii. Facebook, Data Policy, accessed August 8, <https://www.facebook.com/about/privacy/other>
- iv. Google, Privacy Policy, accessed August 8, <https://www.google.com/policies/privacy/>
- v. Google, Transparency Report, accessed August 8, 2017, [https://www.google.com/transparencyreport/userdatarequests/legal-process/#what\\_kinds\\_of\\_data](https://www.google.com/transparencyreport/userdatarequests/legal-process/#what_kinds_of_data)
- vi. Yahoo, Frequently Asked Questions, accessed August 8, 2017, <https://transparency.yahoo.com/faq>
- vii. Microsoft, Law Enforcement Requests Report , accessed August 8, 2017, <https://www.microsoft.com/en-us/about/corporate-responsibility/terr>
- viii. Apple, Legal Process Guidelines - Government & Law Enforcement outside the United States, accessed August 8, 2017, <https://images.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf>

## Appendix II

- i. Twitter, Information requests, July- December 2016, accessed August 8, 2017, <https://transparency.twitter.com/en/information-requests.html> ; Twitter, Guidelines for Law Enforcement, August 8, 2017, <https://support.twitter.com/articles/41949#16>
- ii. Facebook, Government Requests Report, India, July –December, 2016, accessed August 8, 2017, <https://govtrequests.facebook.com/country/India/2016-H2/>; Facebook, Information for Law Enforcement Authorities, accessed August 8, 2017, <https://www.facebook.com/safety/groups/law/guidelines/>
- iii. Google, Transparency Report, India, July- December 2016, accessed August 8, 2017, <https://www.google.com/transparencyreport/userdatarequests/countries/>; Google, Transparency Report, accessed August 8, 2017, <https://www.google.com/transparencyreport/userdatarequests/legalprocess/>
- iv. Yahoo, Transparency Report, India, accessed August 8, 2017, <https://transparency.yahoo.com/government-data-requests/country/India/35/?tid=35> ; Yahoo, Yahoo! Inc. Law Enforcement Response Guidelines, accessed August 8, 2017, <https://transparency.yahoo.com/law-enforcement-guidelines/us>
- v. Microsoft, Law Enforcement Requests Report, accessed August 8, 2017, <https://www.microsoft.com/en-us/about/corporate-responsibility/lerr>
- vi. Apple, Legal Process Guidelines - Government & Law Enforcement outside the United States, accessed August 8, 2017, <https://images.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf>. Apple, Transparency Report, accessed August 8, 2017, <https://www.apple.com/privacy/transparency-reports/>

### About the Authors:

**Bedavyasa Mohanty** is an Associate Fellow with ORF's Cyber Initiative. His current work focuses on encryption and the regulation of lethal autonomous weapons systems. Bedavyasa coordinates ORF's cyber security capacity building for Indian law enforcement officials and is the convenor of CyFy, ORF's flagship conference on cyber security and internet governance. He is a lawyer by training and completed his BA LLB (Hons) from the National University of Juridical Sciences, Kolkata.

**Madhulika Srikumar** is a Junior Fellow with ORF's Cyber Initiative. A lawyer by training, she works at the intersection of policy, law and technology -- specifically how the law can act as both a safeguard against and enabler of emerging technologies. Her current work focuses on the effect of technology on evolving societies - specifically the role of tech in urban mobility and bias in algorithmic decision making. Madhulika previously interned with the Internet & Jurisdiction Project, Paris and the Centre for Communication Governance in NLU-D.

**Observer Research Foundation** (ORF) is a public policy think-tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research and stimulating discussions. The Foundation is supported in its mission by a crosssection of India's leading public figures, academics and business leaders.

Observer Research Foundation  
20, Rouse Avenue Institutional Area,  
New Delhi — 110002  
INDIA

Phone: +91 011 43520020  
Fax: +91 011 43520003  
Email: [contactus@orfonline.org](mailto:contactus@orfonline.org)