OBSERVER RESEARCH FOUNDATION

Cross-Border Requests for Data Project of the Georgia Tech Institute for Information Security and Privacy

INDIA-US DATA SHARING FOR LAW ENFORCEMENT :

BLUEPRINT FOR REFORMS

INDIA-US DATA SHARING FOR LAW ENFORCEMENT :

BLUEPRINT FOR REFORMS

INSTITUTIONS

Observer Research Foundation (ORF) seeks to lead and aid policy thinking towards building a strong and prosperous India in a fair and equitable world. It helps discover and inform India's choices, and carries Indian voices and ideas to forums shaping global debates. ORF provides non-partisan, independent analyses and inputs on matters of security, strategy, economy, development, energy, cyber policy and global governance to diverse decision-makers (governments, business communities, academia, civil society). ORF's mandate is to conduct in-depth research, provide inclusive platforms and invest in tomorrow's thought leaders today.

Cross-Border Requests for Data Project of the Georgia Tech Institute for Information Security & Privacy (IISP) is supported by both the Scheller College of Business and IISP. It is led by Professor Peter Swire, 2018 Andrew Carnegie Fellow and former US White House Chief Counselor for Privacy during the Clinton Administration. The project has been a leading source of research on issues of cross-border government requests for information. In 2018, members of the Project were instrumental in the development of the Cross-Border Data Forum, https://www.crossborderdataforum.org/.

INDIVIDUAL AUTHORS

Madhulika Srikumar is an Associate Fellow and Programme Coordinator with the Cyber Initiative at Observer Research Foundation in New Delhi. She is also a 2019 public interest technology fellow with New America in Washington DC. Her previous research on law enforcement access to data has been cited extensively by prominent stakeholders, including the expert committee established by the government to draft India's first data-protection law. A lawyer by training, Srikumar regularly authors opinion pieces for leading publications. She also convenes the Foundation's annual 'AI For All' dialogue in Mumbai and leads ORF's efforts on AI policy and algorithmic bias, especially the ways in which machine learning can exacerbate existing gender inequities.

Sreenidhi Srinivasan is a Research Faculty Member at Georgia Tech. Her research focuses on cross-border data issues and she has co-authored writings on data access by law enforcement in India, including "Foundations of a Potential Executive Agreement Between India and the US," which was published in the 2018 CyFy Journal. Srinivasan has previously worked as Senior Resident Fellow at the Vidhi Centre for Legal Policy, a New Delhi-based think tank. Srinivasan holds a master's degree in law from Columbia Law School where she focused her programme on privacy and technology.

DeBrae Kennedy-Mayo is a Research Faculty Member at Georgia Tech. Swire and Kennedy-Mayo are the co-authors of the 2018 edition of US Private Sector Privacy: Law and Practice for Information Privacy Professionals, IAPP's book used by those studying for privacy certification. Kennedy-Mayo's first professional paper, entitled "In Search of a Balance Between Police Power and Privacy in the Cybercrime Treaty," was published in 2002. Kennedy-Mayo has spent most of her career working in government, acting as both an Assistant Attorney General for the State of Georgia and as an Assistant District Attorney for several local governments in Georgia.

Peter Swire is Associate Director for Policy of the Institute for Information Security and Privacy (IISP) at Georgia Tech. Swire is the Research Director of the Cross-Border Data Forum. He has been a privacy and cyberlaw scholar, government leader, and practitioner since the rise of the Internet, in the 1990's. Swire is the Elizabeth and Tommy Holder Chair in the Scheller College of Business, with appointments by courtesy with the College of Computing and School of Public Policy. He is senior counsel with the law firm of Alston and Bird LLP.

The authors would like to express their sincere gratitude for assistance in this project from law enforcement and other government officials, industry representatives; and members of civil society, as well as academic and other experts. The research team at Georgia Tech would like to thank Justin Hemmings and Jack Leahey for their work on this paper. The authors are grateful to Samir Saran, President of ORF, for his guidance and to Arun Sukumar and Bedavyasa Mohanty for their inputs.

The authors are grateful for the major funding for this project from the Hewlett Foundation Cyber Initiative. Further information on funding and activities of the Georgia Tech Cross-Border Requests for Data Project is available at http://www.iisp.gatech.edu/cross-border-data-project. ORF's declaration of foreign and domestic contributions is available at https://www.orfonline.org/declaration-of-contributions/.

The views expressed here as well as all errors therein are the authors' alone. For corrections or comments, please email debrae.kennedy-mayo@scheller.gatech.edu.

Designed by: Artlab

US - INDIA COOPERATION AND INFORMATION SHARING FOR LAW ENFORCEMENT PURPOSES

PREFACE: THE VIEW FROM INDIA

This report—through interviews with a multitude of stakeholders, including Indian law enforcement, global communication service providers, current and former government officials, and civil society groups, sets out the law and procedure of cross-border law enforcement access to data between India and United States. The report exhaustively outlines the cooperation between the two states in information sharing for law enforcement purposes and the challenges therein. The authors evaluate the existing bilateral channels for data sharing and the potential for the two countries to enter into a new Executive Agreement to streamline access to communications content.

Indian law enforcement has for years been setting off alarm bells about the challenges of legitimate cross-border access to data. With popular device manufacturers and social media platforms incorporated in the United States, foreign law enforcement requests, must meet the requirements under US law to gain access to electronic data during investigations. When investigating routine crimes with a cyber element or crimes online, police officials are forced to rely on a long and arduous bilateral process with the US government to obtain electronic evidence from US communication providers. After many years, 2018 finally saw the executive take decisive steps towards addressing the issue.

Three big developments over the past year are at the centre of this policy shift and have contributed to the mainstreaming of the issue. First, the spread of false news on WhatsApp that instigated lynch mobs and resulted in 27 reported deaths, drove home the sobering reality of Indian law enforcement's inability to access the origins of messages sent over an encrypted medium.[1] Where data is strongly encrypted, a wiretap does not provide any police access to the content.[2] This episode further highlighted the urgency of creating reliable channels for information-sharing between foreign service providers and local investigating agencies.

The spread of false news on WhatsApp that instigated lynch mobs and resulted in 27 reported deaths, drove home the sobering reality of Indian law enforcement's inability to access the origins of messages sent over an encrypted medium.

Second, the controversy surrounding Paytm's practices (a popular mobile wallet in the country) on allegedly disclosing user data to the government without following due process, brought not just company practices into focus but also underscored deeper problems with the existing law.[3] Law enforcement in India, when requesting user data from online intermediaries or social media companies, relies on the longstanding framework under the Code of Criminal Procedure, 1973 (CrPC), which does not mandate judicial authorisation for data requests.

1 Timothy Mclaughlin, "How Whatsapp Fuels Fake News And Violence In India", Wired (Dec. 12, 2018), https://www.wired.com/story/how-whatsapp-fuels-fake-news-and-violence-in-india/

2 Peter Swire, "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud," 2 International Data Privacy Law 200 (2012), SSRN: https://ssrn.com/abstract=2038871.

3 Madhulika Srikumar, "This Isn't Just About Paytm – Laws on Government Access to Data Need to Change", The Wire (May. 28, 2018), https://thewire.in/law/paytm-data-theft-cobrapost-sting

And finally, calls for data localisation, i.e. mandating companies to store data locally to legally operate in the country, manifested in a variety of regulations and policies introduced by different arms of the government in the past year.[4] Notably, the committee established by the govern ment to frame India's first data protection law, headed by former Supreme Court judge B.N. Srikrishna, imposed a requirement on all data fiduciaries to store data in the country either exclusively or in the form of mirror servers.[5] The primary concern cited by the Committee for this policy shift was to ease law enforcement efforts to access information required for criminal investigations and evidence-gathering for prosecutions.[6] The recently published draft amendments to the Information Technology Act [Intermediary Guidelines (Amendment) Rules, 2018] by the Ministry of Electronics and Information Technology (MeitY) further reveal the government's intent to introduce strong legislation aimed at regulating online intermediaries and assisting law enforcement, even at the cost of potentially compromising encryption.[7]

These developments firmly indicate that reforms are deeply necessary in law enforcement access to data to ease extant conflicts of laws, institute privacy-protecting safeguards, and discourage further fragmented policy approaches through data localisation.

Currently, the Electronics Communications Privacy Act (ECPA) bars US-based service providers from disclosing electronic communications to any law enforcement entity—US or non US—unless requirements under US law are met. The request for user data from Indian law enforcement, therefore, needs to meet the US legal standard that there is "probable cause" that a crime has occurred and that contraband or evidence of the crime will be found by during the search. These US legal requirements apply even though the crime has occurred outside the US, the victim and suspect are not US persons, and the electronic evidence is being requested by foreign law enforcement. Under existing law, Indian law enforcement place relis on a bilateral mechanism through the India-US Mutual Legal Assistance Treaty (MLAT) to transmit requests for user data. This process has often been criticised for being outdated and time consuming and by some

---

4 Payments: The Reserve Bank of India (RBI) issued a notification requiring all "payment system providers" to store all payments data only in India. Payment system providers includes a wide spectrum of actors including international card networks such as MasterCard, and even operators of pre-paid wallets such as Google Pay and WhatsApp payments. Reserve Bank of India Notifications, "Storage of Payment Systems Data", (Apr. 6, 2018), https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0.

Privacy: The draft Personal Data Protection Bill, 2018 places restrictions on cross-border transfer of data requiring every data fiduciary to store a mirror-copy in the country with collectors of "critical personal data" required to process data only in servers located in India. Personal Data Protection Bill, 2018, http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

E-commerce: Leaked copy of the draft national e-commerce policy indicates imposing mandatory data localisation requirements on all e-commerce platforms including social media and search engines to store "data generated by users in India" locally. The policy also indicates potentially incentivising players to store data in India through tax waivers. Electronic Commerce in India: Draft National Policy Framework, https://www.medianama.com/wp-content/uploadsDraft- National-E-commerce-Policy.pdf.

Cloud: Proposed national cloud policy is likely to recommend localisation of cloud data generated in India. Currently, the Ministry of Electronics and Information Technology (MeitY) requires all government departments using cloud services (from empanelled providers) to ensure that all data is stored within the country. Aditya Kalra, "Exclusive: India panel wants localisation of cloud storage data in possible blow to big tech firms", Reuters (Aug. 4, 2018), https://in.reuters.com/article/us-india-data-localisation-exclusive/exclusive-india-panel-wants-localization-of-cloud-storage-data-in-possible-blow-to-big-tech-firms-idINKBN1KP08J, "MeitY issues guidelines requiring all cloud data storage used by the government to be within the country", Firstpost, (Jun. 1, 2017), https://www.firstpost.com/tech/news-analysis/meity-issues- guidelines-requiring-all-cloud-data-storage-used-by-the-government-to-be-within-the-country-3703763.html.

5 Sections 40 and 41, The Personal Data Protection Bill, 2018, categories of personal data identified as critical personal data can only be processed in a server or data centre located in India.

6 Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians", 27 July 2018.

7 Section 5 of the The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 states that, "When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised."

estimates from Indian sources takes as long as three years and four months on average to complete.[8] On the other hand, direct requests to companies for basic subscriber information (BSI) and transactional data are not barred by ECPA, although in practice there is inconsistent access, potentially harming law enforcement and users' interests.

The recently passed US Cloud Act (Clarifying Lawful Overseas Use of Data Act) for the first time enables foreign law enforcement to request electronic content directly from US service providers under an Executive Agreement with the US government. As part of the Executive Agreement, the foreign country must ensure adequate levels of procedural protections for crimes covered under the Agreement. The Cloud Act provides a much-needed framework to ease cross-border access to data, not only speeding up any future process but safeguarding user privacy, and alleviating existing concerns around lacking capacity. Such a direct-data sharing regime under an Executive Agreement will, therefore, not only address law enforcement concerns but also strengthen the overall case against mandatory data localisation.

Data localisation, while often touted as a solution to law enforcement's data needs, will not bring about any increased compliance on the part of companies when responding to requests from law enforcement. ECPA still effectively bars US companies from disclosing user data to foreign law enforcement in the absence of American legal standards being met. Therefore, regardless of where the data is located, US service providers are still be bound by US laws. However, a data sharing agreement under the US Cloud Act will shift the locus to the domestic law of the requesting country, and compliance with the Executive Agreement, thereby ensuring that US companies respond to legally valid requests for content.

The Cloud Act presents an opportunity to not only resolve conflicts of law but also harmonise enforcement regimes across jurisdictions, not limited to India and the United States alone.

The Cloud Act presents an opportunity to not only resolve conflicts of law but also harmonise enforcement regimes across jurisdictions, not limited to India and the United States alone. The European Commission's E-evidence proposal puts forth a similar model where judicial authorities in one Member State can obtain evidence directly from service providers located in other Member States.[9] This model is of special significance to India where law enforcement comes up short while handling crimes involving transnational elements such as online radicalisation and cyber-crime. These crimes often involve accounts and individuals spread out across the globe and therefore merely localising data belonging to Indian citizens will not aid law enforcement investigations.

Finally, for any law enforcement request to be eligible under the Cloud Act Executive Agreement, they will need to adhere to privacy protecting safeguards – such as being specific about the information sought, being based on "articulatable and credible facts," and being subject to independent oversight. This model will ensure that requests are bound by a higher threshold of privacy and due process than they currently are.

Under existing law, requests are either directly issued by law enforcement officers[10] or in cases of interception are authorised by and subject to executive review. In the aftermath of the Supreme Court's judgment in Puttuswamy, however, some of these provisions may stand to be revised.[11] For instance, the executive authorisation for interception that, which does not allow for

8 Neha Alwadhi, "CBI & FBI join hands to reduce time required to fulfil requests on information and evidence", The Economic Times, 7 December 2015, https://economictimes.indiatimes.com/news/politics-and-nation/cbi-fbi-join-hands-to-reduce-time-required-to-fulfil-requests-on-information-and-evidence/articleshow/50069794.cms.

9 Theodore Christakis, "Big Divergence of Opinions on E-Evidence in the EU Council," Cross-Border Data Forum, 22 October 2018, https://www.crossborderdataforum.org/big-divergence-of-opinions-on-e-evidence-in-the-eu-council-a-proposal-in-order-to-disentangle-the-notification-knot.

10 Section 91, The Code of Criminal Procedure, 1973

11 K.S. Puttuswamy v. Union of India, 2017 (10) SCALE 1)

any inter-branch oversight, may not meet the "necessary and proportionate" test for imposing restrictions on privacy. India must therefore necessarily move towards a judicial sanction model for requesting communications data to qualify for an Executive Agreement with the US under the Cloud Act, as well as to meet European law standards.

This paper proposes two mechanisms that together can help India qualify for this Executive Agreement. First, for individual data requests, the paper proposes resorting to existing provisions under the CrPC that allow judicial authorisation. And second, to build institutional safeguards, including for data collection and processing, 'qualified entities' should be established that are specifically tasked with handling sensitive data obtained for law enforcement processes.

This paper builds on prior research conducted by the Cross-Border Requests for Data Project of the Georgia Tech Institute for Information Security & Privacy and the Observer Research Foundation's Cyber Initiative.

This paper builds on prior research conducted by the Cross-Border Requests for Data Project of the Georgia Tech Institute for Information Security & Privacy[12] and the Observer Research Foundation's Cyber Initiative. It does not delve extensively into the substantive and procedural failings of the MLAT process. Instead, it dissects existing laws in India and the US that have a bearing on the legitimate rights of law enforcement to access communications data. The paper explores the institutional and legal changes necessary for a direct-data sharing agreement between India and the US that can address not just immediate law enforcement concerns but also potentially act as a primer for harmonisation of data-sharing regimes worldwide.

12 http://www.iisp.gatech.edu/cross-border-data-project.

EXECUTIVE SUMMARY

This paper proposes what appears to be a workable path to an India-US Executive Agreement under a new US law known as the Cloud Act. A major rationale for current data localisation proposals in India is to address the difficulties encountered by Indian law enforcement in accessing content held by US service providers. If a carefully crafted Executive Agreement based on the principles outlined in this paper could be adopted, this rationale for data localisation would be greatly weakened.

Observer Research Foundation (ORF) and Cross-Border Requests for Data Project of the Georgia Tech Institute for Information Security & Privacy have joined forces to write this report. The authors have collaborated to gather perspectives from both India and the US and to provide a holistic view of India-US cooperation for law enforcement. The report provides an overview of the two legal systems at issue, the existing types of cooperation and information sharing, and potential options for an Executive Agreement under the US Cloud Act.

The key takeaways from this paper:

- *The Problem* – Law enforcement in India currently face problems accessing electronic evidence, primarily the content of emails and social media communications, where the services are provided to Indian customers by US service providers.

- *The Current Process* – Two formal request mechanisms exist between India and the US for content of stored electronic communications: MLAT and letters rogatory.

- *The Current Collaborations* – Numerous mechanisms exist for cooperation and information sharing outside of formal MLA.

- *The Proposal* – This Report proposes what appears to be a workable path to an India-US Executive Agreement to streamline access to content of stored electronic communications for serious crimes.

- *The Hurdles* – Significant practical and political hurdles exist to successfully negotiating an India-US Executive Agreement.

- *The Hope* – Although we recognise that the road to an Executive Agreement between India and the US would be complex, we believe that the effort is worthwhile for India itself, and as a model for addressing many nations' problems posed by the globalisation of criminal evidence.

The Problem **- Law enforcement in India currently face problems accessing electronic evidence, primarily the content of emails and social media communications, where the services are provided to Indian customers by US service providers.**

1. *The globalisation of criminal evidence has created a basic problem for law enforcement worldwide, including Indian law enforcement.*

With the rise of online content such as social media and webmail, many people conduct communications via electronic service providers such as Apple, Facebook, Google, Instagram, Microsoft, and Snapchat – all US companies. Emails, social media communications, and other electronic evidence are typical in modern criminal investigations. Non-US law enforcement entities currently can legally gain access to electronic communications content held by US service providers, but only through time-consuming mechanisms that require foreign law enforcement requests to meet the requirements of US law.

2. *In the US, the Electronics Communications Privacy Act (ECPA) does not allow US service providers to release electronic communications to any person, with only narrow exceptions.*

The US law known as ECPA prohibits service providers in the US from disclosing the content of communications to law enforcement except through a warrant or an appropriate request through a formal request mechanism such as MLAT. Service providers risk civil and criminal penalties if they release data in violation of ECPA.

a. Under the US legal standard, a request needs to show "probable cause" - despite the fact that the crime occurred outside the US, the victim and suspect are not US persons, and the electronic evidence is being requested by foreign law enforcement.

b. The"probable cause" standard is stricter than non-US practice before a government can access evidence.

3. *Our interviews in India found concerns that there was an overall lack of cooperation from the US. This lack of cooperation from the US was perceived to result in delays in receiving access to stored electronic communications.*

a. From our research, two key factors influence the delays experienced by Indian law enforcement.

i. The sheer volume of requests coming from India, with its population of well over a billion people, slows the review processes between the two governments.

ii. Indian law enforcement must comply with both Indian and US legal requirements to access stored electronic communications held by service providers in the US. Law enforcement in India may understandably lack training to ensure compliance with complex legal requirements in the US for release of electronic communications by service providers.

- The report explains the legal standards for access to content of stored electronic communications in both India and the US.

4. The stakes are high if additional cooperation between India and the US is not possible.

Notably, arguments for data localisation can become more persuasive if India lacks access to important evidence concerning serious crimes. As of the writing of this report, the Indian government is considering a bill that would require data localisation for most types of businesses.

The Current Process - **Two formal request mechanisms exist between India and the US for content of stored electronic communications.**

1. *The MLAT process, the most commonly used formal request mechanism, takes an estimated average of at least 10 months (global average) for law enforcement to receive electronic evidence.*

An MLAT is a formal agreement between countries to seek and exchange evidence located in their jurisdictions upon requests from another country that is party to the treaty.

2. *The letters rogatory process, a lesser known formal request mechanism involving the courts in each country, is believed to take longer than the MLAT process.*

A letters rogatory process enables a court to issue letters of request to foreign courts or authorities for compelling production of a document. Current ambiguity in Indian law leads some to believe that the law only permits the usage of letters rogatory – the lengthier of the two processes.

The Current Collaborations - **Mechanisms already exist for cooperation and information sharing outside of MLA.**

1. *Methods currently available for cooperation and information sharing between India and US service providers.*

a. Along with other mechanisms, US service providers may legally respond to requests from non-US law enforcement for non-content data such as subscriber information and metadata.

2. *Methods currently available for bilateral and multilateral cooperation and information sharing involving India and the US include:*

a. The US Legat Office;

b. Efforts to combat cyber crime;

c. Counterterrorism efforts and other intelligence and military sharing;

d. Efforts to combat money laundering and other financial schemes; and

e. INTERPOL.

The Proposal – **This Report proposes what appears to be a workable path to an India-US Executive Agreement to streamline access to content of stored electronic communications for serious crimes.**

1. *Executive Agreements under the US Cloud Act must meet requirements for individual requests and for institutional protections.*

The Cloud Act, 18 U.S.C. § 2523, contains the new provision for Executive Agreements. Where an Executive Agreement is in effect, countries such as India would be able to go directly to service providers for stored content, without the need to use the MLAT process and get approval from a US judge that probable cause exists.

a. ***Each request under an Executive Agreement must afford "robust substantive and procedural protections for privacy and civil liberties":***

- *Requests be subject to independent review.* The request "shall be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order."

- *Particularised requests.* The request must target a specific person, account, address, personal device or other identifier. That is, the request cannot be for bulk collection of data or for a general warrant.

- *Serious crimes.* The request "shall be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism."

- *Comply with domestic law.* The request shall comply with the domestic law of the country - in this case, India.

- *Requests based on "articulable and credible facts."* The request must show a clear factual basis for the individual request. This standard is less strict than the typical US standard of probable cause of a crime.

- *Prohibition on the use of data to infringe on freedom of speech, as well as requiring countries to meet human rights standards, such as a prohibition on torture.*

b. ***The Executive Agreement must have institutional protections in place to qualify under the Cloud Act.***

- Notably, these protections include: a prohibition on direct or indirect targeting of US person data; procedures to minimise the data received; and a mechanism in place to enable review of the country's compliance with the Cloud Act requirements every five years.

2. *We propose two innovative mechanisms, available under existing Indian law, that would together address some major concerns about whether India can qualify for a Cloud Act Executive Agreement.*

One mechanism would meet the Cloud Act requirements for individual law enforcement requests. The second mechanism would meet the Cloud Act requirements for institutional safeguards applying to law enforcement requests.

a. ***The first proposed mechanism would make a law enforcement request eligible under the Executive Agreement where a judge issues the order that meets the Cloud Act requirements, as is already available under Indian law.***

This first proposal involves how India may leverage existing legal procedures in order to meet the Cloud Act requirements for each individual request.

- Indian law does not generally require: judicial approval; detailed specificity in a court order; or a finding that a request has met a standard such as articulable and credible facts. These three types of safeguards, however, are expected elements under the Cloud Act for an individual request for content.

- The idea we propose is straightforward – existing law in India authorises those stricter procedures, even though the stricter procedures are not required. A Cloud Act request, therefore, may proceed when the stricter, optional procedures are followed, likely without the need to pass new Indian legislation.

b. The second proposed mechanism would identify "Qualified Entities" for Cloud Act requests–one or more designated agencies within India would set up institutional mechanisms to ensure compliance with the Cloud Act.

The general institutional requirements under the Cloud Act is that a government such as India must have "clear legal mandates and procedures governing those entities of the foreign government that are authorised to seek data under the Executive Agreement, including procedures through which those authorities collect, retain, use, and share data, and effective oversight of these activities."

- One key point in our proposal is to highlight the importance of selecting an appropriate Qualified Entity that would be designated in an India-US Executive Agreement.

- The Executive Agreement can name India's existing central authority for MLATs, the Ministry of Home Affairs (MHA)[13], as a Qualified Entity.

- The newly formed Cyber and Information Security Division (C&IS) under the MHA, set up in November 2017, appears best placed to adopt the role of a Qualified Entity.

- It is our proposal that a separate committee be formed either under the Indian Cyber Crime Coordination Centre (I4C) subdivision or under the overall C&IS division to route user data requests to US service providers directly and to meet the institutional requirements under the Cloud Act Executive Agreement.

- The committee can be headed by a Director of IG rank (Inspector General of Police) and a Deputy Director of DIGP rank (Deputy Inspector General of Police). Officers of the Inspector or Sub Inspector ranks from state law enforcement agencies can be permanently appointed to the committee on a rotational basis. Four or more officers of the Deputy Superintendent of Police (DSP) rank who are specifically trained, could either be designated as zonal heads (representing the four different regions) or as subject-matter leads in priority areas including counterterrorism, cyber incidents and anti-money laundering. . Further, the MHA and the Ministry of External Affairs (MEA) can appoint a member at the Joint Secretary level to coordinate not just outgoing but also incoming requests under the Executive Agreement.

The Hurdles **- Significant practical and political hurdles exist to successfully negotiating an India-US Executive Agreement.**

1. From a practical standpoint, the tremendous judicial backlog in India would be but one example of concerns to be raised by those in the country.

Requiring judicial oversight for production of evidence would add to the burden on the court system.

13 However, for implementing MLAT requests to date, our interviews found some concern that MHA has not been heavily staffed previously. There is thus some question about whether MHA, a ministry that is known to be burdened with various responsibilities, would receive the resources and institutional commitment needed to meet the institutional requirements described in the previous section.

2. *Politically, such an Executive Agreement faces obstacles in both countries.*

a. Based on the US authors' experience, it will be difficult for the US to bring an Executive Agreement with India into effect unless there are good answers for privacy and civil liberties concerns.

b. In India, data localisation is being debated at the writing of this report. Passage of data localisation legislation would appear to contradict the Cloud Act requirements that the non-US country should demonstrate "a commitment to promote and protect the global free flow of information" and the "open, distributed, and interconnected nature of the Internet."

The Hope - We recognise that the road to an Executive Agreement between India and the US would be complex. Because the issues faced in India are experienced by many other countries around the world, we believe that the effort is worthwhile in India itself and as a model for progress to be made on many nations' problems posed by the globalisation of criminal evidence.

INTRODUCTION: CURRENT CHALLENGES

Law enforcement in India currently face problems in accessing the content of emails and social media communications, where these services are provided to Indian customers by US service providers.[14] This report examines the range of currently available avenues for law enforcement cooperation and information-sharing, and explores potential avenues for law enforcement to directly access content held by US service providers under a new US law known as the Cloud Act.

The globalisation of criminal evidence has created a basic problem for law enforcement worldwide, including Indian law enforcement.[15] With the rise of online content such as social media and webmail, many people conduct communications via electronic service providers such as Apple, Facebook, Google, Instagram, Microsoft, and Snapchat, all US companies. Emails, social media communications, and other electronic evidence are typical in modern criminal investigations.[16] Currently, non-US law enforcement entities can gain access to electronic communications content held by US service providers,[17] but only through time-consuming mechanisms[18] that require that foreign law enforcement requests meet the requirements of US law.

The globalisation of criminal evidence has created a basic problem for law enforcement worldwide, including Indian law enforcement.

In the US the Electronics Communications Privacy Act (ECPA)[19] does not allow US service providers to release electronic communications to any person, with only narrow exceptions.[20] One such exception enables law enforcement entities to require US service providers to

14 This difficulty faced by law enforcement in accessing the content of electronic communications is one of the arguments put forth by proponents of data localisation.

15 The topic of the globalisation of criminal evidence is a main topic of research for the Georgia Tech team involved in this report. For an overview of the topic, view the article published by the International Association of Privacy Professional's entitled "The Globalization of Criminal Evidence." Jennifer Daskal, Peter Swire, and Theodore Christakis, "The Globalization of Criminal Evidence," IAPP, 16 October 2018, https://iapp.org/news/a/the-globalization-of-criminal-evidence/. For details of further research by Georgia Tech, see the website titled "Cross-Border Requests for Data Project" hosted by the Institute for Information Security & Privacy, http://www.iisp.gatech.edu/cross-border-data-project. An additional online resource which the authors at Georgia Tech helped to create is the Cross Border Data Forum. https://www.crossborderdataforum.org/.

16 This report is focused on stored communications, not real-time interception. Traditionally, protections related to real-time interception—known in the past as "wiretaps" —have been more stringent than safeguards for stored communication. With the advent of the Internet, the practical reality is that an email in transit (which would require real-time interception) becomes a stored email (with only the protections of stored communications) within a fraction of a second.

17 The term "electronic communication service provider" is defined broadly under the US Electronic Communications Privacy Act. For a discussion on the breadth of the term, see Chapter 9 of "Swire Testimony in Landmark EU Privacy Case," Expert to the Irish High Court in Irish Data Protection Commissioner v. Facebook and Max Schrems, 7 February 2017, https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony.

18 The current formal mechanisms used between India and the US are Mutual Legal Assistance (MLA) requests and letters rogatory. These two mechanisms are discussed in detail in Chapter IV of this report.

19 The Electronic Communications Privacy Act is a federal law in the US governing interception and access to stored data by law enforcement. This report is focused on stored communications.

20 18 U.S.C. 2702(a)(1) and (2), https://www.law.cornell.edu/uscode/text/18/2702.

disclose the content of communications through appropriate legal processes. ECPA applies varying legal standards to different categories of electronic evidence, with lower protections for categories that reveal less information about the user (so require less protection against potential abuses by law enforcement) and higher protections when the information reveals intimate details about the user (so potential violations by law enforcement would be more intrusive). An example on the lower end of the spectrum is the category known as basic subscriber information (BSI).[21] Under ECPA, law enforcement can gain access to a user's BSI by meeting fairly minimal protections of the user's privacy, typically by obtaining a subpoena.[22] On the higher end of the spectrum is the category of the content of electronic communications. For law enforcement to access the content of electronic communications under ECPA, the legal requirements under US law are string—a judge must approve the request and that approval will only be given when law enforcement has met the US standard known as "probable cause."[23]

As of 2018, the treatment of the categories that fall between BSI and content—known as categories of non-content electronic communications—is more complex and less certain under US law.[24] The 2018 decision in the US Supreme Court case of Carpenter v. United States required a probable cause warrant for a particular type of location data, moving at least one category of non-content electronic communications into the higher end of the spectrum.[25] Another of these categories often requested in criminal investigations is "traffic data." This category includes the sender and the recipient of the electronic communications as well as the date and time of the communication. Carpenter does not explicitly state the standard for traffic data.

To address the uncertainty related to categories of non-content electronic communications that are not specifically enumerated in Carpenter, we turn to the practices of businesses implemented after the Court's decision. According to Apple's current policy for law enforcement, the company requires a middle level of protection for the following types of non-content data: FaceTime call invitation logs; Find My iPhone transactional activity; Game Centre transactional records and / or

---

21 BSI is defined as the identifying information for the owner or controller of an Internet service account. BSI can include the name, address, and any assigned number or identity such as a phone number, username, IP address, or email address. 18 U.S.C. § 2703(c), https://www.law.cornell.edu/uscode/text/18/2703.

22 A subpoena is a court order, signed by a judge, requiring a witness produce certain documents in question. The standard for acquiring a subpoena is relatively low. 18 U.S.C. § 2703, https://www.law.cornell.edu/uscode/text/18/2703; see e.g. Subpoena, ECPA Legal Process Glossary, Transparency Report, https://transparencyreport.google.com/user-data/overview?hl=en_GB. Note that under certain circumstances, service providers can voluntarily provide BSI to law enforcement. See 18 USC § 2702, https://www.law.cornell.edu/uscode/text/18/2702. It is also worth noting that, under current US law, metadata can be voluntarily provided by the service provider to foreign law enforcement. See 18 USC § 2702(c)(6); 18 U.S.C. § 2711(4); see also Greg Nojeim, "MLAT Reform Proposal: Protecting Metadata," Lawfare, 10 December 2015, https://www.lawfareblog.com/mlat-reform-proposal-protecting-metadata.

23 Chapter II of this Report provides in-depth discussion of the requirements under US law, including the concept of "probable cause."

24 See Convention on Cybercrime of the Council of Europe (referred to as the Budapest Convention), (defining "traffic data" as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service," https://www.coe.int/en/web/cybercrime/the-budapest-convention; see also "Criminal Justice Access to Data in the Cloud: Challenges," Council of Europe Cybercrime Convention Committee, 2015, https://rm.coe.int/1680304b59.

25 In Carpenter, the US Supreme Court held that law enforcement officers are required to obtain a judge-issued search warrant, based on probable cause, prior to accessing cell-site location information. Carpenter v. US, US Supreme Court Slip Opinion, October Term 2017; https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf. Prior to this 2018 decision, this type of location – like other non-content data – required a lower standard of protection under the US Constitution; See Kimberly Peretti, Kawrence Sommerfeld, and Nameir Abbas, "US Supreme Court Builds on Individuals' Private Rights," Alston & Bird, 26 July 2018, https://www.alston.com/en/insights/publications/2018/07/us-supreme-court-builds-on-individuals-privacy; David Kris, "Carpenter's Implications for Foreign Intelligence Surveillance," Lawfare, 24 June 2018, https://www.lawfareblog.com/carpenters-implications-foreign-intelligence-surveillance.

records of the specific games accessed; iTunes purchase/download transactional records; mail logs;iMessage capability query logs; iTunes purchase/download transactional records; and transactional records for My Apple ID and iForgot logs.[26] Facebook's policy specifically identifies two categories of non-content electronic communication that require a middle level of protection:[27] "message headers" and "IP addresses."[28] These policies of service providers suggest that these companies currently do not view traffic data as requiring a search warrant.

A simple example shows how the globalisation of evidence affects even routine criminal investigations. Consider a burglary that takes place in Delhi with an Indian suspect and an Indian victim. ... For Indian law enforcement to access this electronic evidence, they must comply with both Indian and US law.

A simple example shows how the globalisation of evidence affects even routine criminal investigations. Consider a burglary that takes place in Delhi with an Indian suspect and an Indian victim. In investigating the crime, Indian law enforcement seeks emails held by a US-based email service provider.[29] For Indian law enforcement to access this electronic evidence, they must comply with both Indian and US law. The current mechanisms for accessing content require multi-step review processes in two governments: the government of the requestor and the government of the country where the request is being sent.

The typical route for transfers of electronic evidence between two countries is a "Mutual Legal Assistance" an MLA request. Under an MLA framework, law enforcement in one country (such as India) requests evidence held in another country (such as the US) for criminal prosecution, frequently pursuant to a Mutual Legal Assistance Treaty an MLAT. In this example, the Indian law enforcement entity in Delhi investigating the burglary would file an MLAT request for review by the Indian Ministry of Home Affairs (MHA). The MHA would then relay the approved request to the Office of International Affairs in the US Department of Justice (DOJ). The US DOJ would then review the request and, once approved, forward the request to a prosecuting attorney. After review, this prosecuting attorney would bring the request from the Indian law enforcement entity in Delhi before a US federal judge. If the judge determined that the Indian request met the relevant US legal requirements, the judge would issue an order requiring the production of the documents by the US service provider. The company would then produce the specified content, which would then be reviewed by the US DOJ to ensure compliance with US laws. The US DOJ would next release the permitted content to MHA in India. Finally, MHA would provide the content to the Delhi police.[30] This process takes a reported estimated average of at least 10 months from start to finish.

---

26 The level of protection required for these two categories is a court order issued pursuant to 18 U.S.C. §2703(d) – known as (d) orders. See e.g. ECPA Court Orders, ECPA Legal Process Glossary, Transparency Report, https://transparencyreport.google.com/user-data/overview?hl=en_GB. Note that under certain circumstances, service providers can voluntarily provide BSI to law enforcement. See 18 U.S.C. § 2702. Legal Process Guidelines: Government and Law Enforcement Within the United States, Apple, 5 December 2018, https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf.

27 The level of protection required for these two categories is a court order issued pursuant to 18 U.S.C. §2703(d) – known as (d) orders. Information for Law Enforcement Authorities, Facebook, https://www.facebook.com/safety/groups/law/guidelines/.

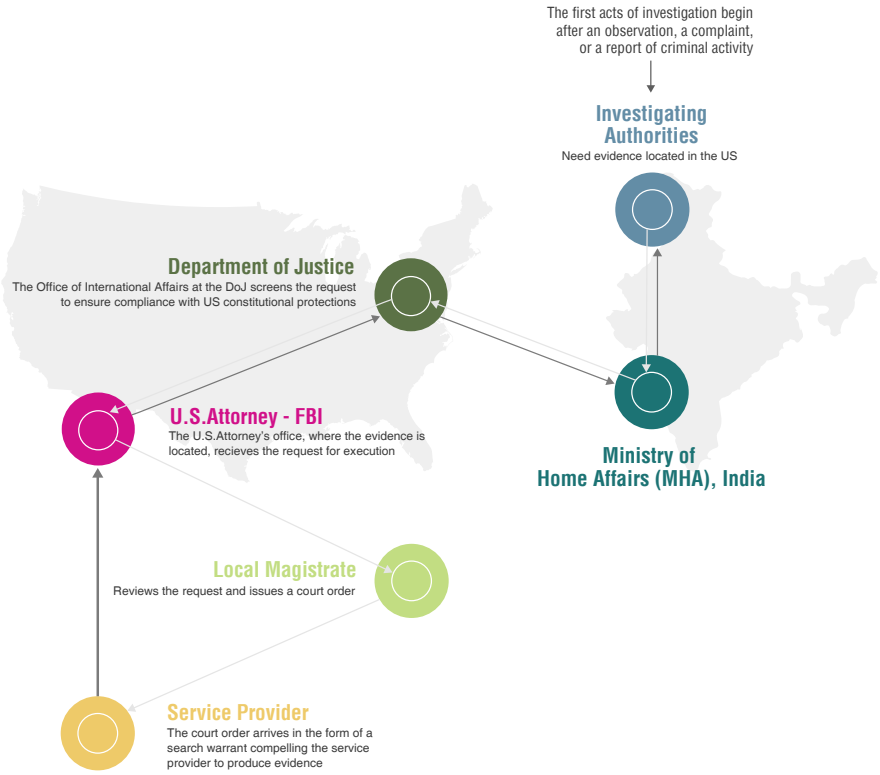
28 As to the changes brought about by Carpenter, Facebook's policy takes an approach that broadly interprets the new category as "location information." Information for Law Enforcement Authorities, Facebook, https://www.facebook.com/safety/groups/law/guidelines/.

29 A similar example, with France as the primary country for comparison, is discussed in Peter Swire, Justin Hemmings and Suzanne Vergnolle, "A Mutual Legal Assistance Case Study: The United States and France" Wisconsin International Law Journal 34, no. 323 (2017), http://hosted.law.wisc.edu/wordpress/wilj/files/2017/12/Final_Proof2.3.15.17.pdf.

30 Bedavyasa Mohanty and Madhulika Srikumar, "Hitting Refresh: Making India-US Data Sharing Work," ORF, 9 August 2017, https://www.orfonline.org/research/hitting-refresh-india-us-data-sharing-mlat/.

In India, the process of requesting electronic evidence is further complicated due to an uncertainty under Indian law about the legality of the MLAT process. Our interviews found that some law enforcement agencies within India believe they must use an even lesser known legal process known as "letters rogatory" – a diplomatic approach where the courts in one country issue letters of request to foreign courts. This avenue also requires multiple levels of reviews in both the requesting and receiving countries (e.g., India and the US) It is worth noting that the recipients involved with this process are under no treaty obligations to review or process letters rogatory, in contrast to the commitments made in MLATs. We are aware of no public statistics related to letters rogatory, but our interviews indicate that the process is even slower than MLATs.

With regard to the delay that Indian law enforcement face in obtaining the content of stored communications, our interviews found a concern that Indian law enforcement wait longer for electronic evidence from US service providers than law enforcement from other countries, and a further concern that the US denies Indian law enforcement access to such evidence more often than in other countries.[31] From our research, two key factors influence these current outcomes. First, the sheer volume of requests coming from India slows the review processes between the two governments. The number of requests originating from India has grown significantly in the past few years. While in the first half of 2013, Facebook received 3,245 requests from India, in 2018 (January to July), it received 16,580 requests.[32] Similarly, Google received 2,691 requests from India in the first half of 2,013 and the number has gone up to 5,105 in the first half of 2018.[33] Twitter



The authors thank Marie Le Pichon and Suzanne Vergnolle for creating the original diagram for the US side of the MLAT Request, which is used here with their permission. The original diagram appeared in Vergnolle's chapter entitled, "Understanding the French Criminal Justice System as a Tool for Reforming International Legal Cooperation and Cross-Border Data Requests," which was published in Data Protection, Privacy, and European Regulation in the Digital Age (Helsinki University Press, 2016).

---

31 For the period January – July 2018, Facebook received 16,580 requests from India out of which in only 53% of instances, Facebook responded with some data. In contrast, the UK made a total of 7,981 requests and some data was produced in 91% of those instances. Mexico received data in response to 77% of requests, Argentina in 73% of the cases, and Canada in 88%. "Government Requests for User Data," Facebook Transparency Report (2018), https://transparency.facebook.com/government-data-requests.

32 Government Requests for User Data – India, Facebook Transparency Report (2018), https://transparency.facebook.com/government-data-requests/country/IN

33 Requests for User Information, Google Transparency Report (2018), https://transparencyreport.google.com/user-data/overview?hl=en.

received a total of 24 requests in 2013 while in the first half of 2018, that figure has risen to 355.[34] This is largely due to the growing number of Internet users in India. As of the writing of this report, the population of India is estimated at 1.3 billion people.[35] The number of Internet users in India is estimated to be around 500 million – second in the world only to China in the number of people online.[36] As an example of social media usage, Facebook has more than 270 million users in India.[37] These statistics suggest that the number of requests made each year by Indian law enforcement to the US can only be expected to increase. Second, India has law enforcement agencies both at the state and federal level. Most investigations are routinely carried out by state police officers with some special crimes being handled by specialised federal agencies. As the earlier example of a burglary illustrated, many crimes with no other international component involve electronic evidence held by a US service provider. It is understandable that state police officers, or any non-US law enforcement officers for that matter, often would not fully know the US legal requirements for a successful request. Even federal law enforcement in India may lack training to ensure compliance with foreign legal requirements.[38]

Regardless of whether a request from Indian law enforcement is submitted via MLAT request or the letter rogatory, the request would need to show "probable cause" (the US legal standard), despite the fact that the crime occurred outside the US, the victim and suspect are not US persons, and the electronic evidence is being requested by foreign law enforcement. The "probable cause" standard is stricter than non-US practice before a government can access evidence.[39]

Regardless of whether a request from Indian law enforcement is submitted via MLAT request or the letter rogatory, the request would need to show "probable cause" (the US legal standard), despite the fact that the crime occurred outside the US the victim and suspect are not US persons, and the electronic evidence is being requested by foreign law enforcement.

34 India Information Requests, Twitter Transparency Report (2018), https://transparency.twitter.com/en/countries/in.html.

35 India Population 2018, World Population Review, http://worldpopulationreview.com/countries/india-population/.

36 Internet Usage in India – Statistics and Facts. Statista, https://www.statista.com/topics/2157/internet-usage-in-india/; see Ranjani Ayyar, "Number of Indian Internet Users Will Reach 500 Million by June 2018, IAMAI Says," The Times of India, 20 February 2018, https://timesofindia.indiatimes.com/business/india-business/number-indian-internet-users-will-reach-500-million-by-june-2018-iamai-says/articleshow/62998642.cms.

37 To put this in context for a US reader, the entire population of the US is approximately 325 million people. This means that the number of Facebook users in India is comparable to the entire population of the US Facebook Revenue and Usage Statistics (2018), Business of Apps, 4 May 2018, http://www.businessofapps.com/data/facebook-statistics/; Donna Rivera, "Facebook Now Has More Users in India than in Any Other Country," Investopedia, https://www.investopedia.com/news/facebook-now-has-more-users-india-any-other-country/. See "India Among Top 5 Countries Seeking User Info from Google," The Times of India, 19 October 2016, https://timesofindia.indiatimes.com/india/India-among-top-5-countries-seeking-user-info-from-Google/articleshow/54848297.cms. According to Statista, India leads the world in the number of Facebook users. Statista, https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/.

38 It may be noted here that requests made by US law enforcement to service providers also sometimes do not receive responses. Scholars have emphasised the need for enhancing training at all levels of law enforcement within the US See William A. Carter and Jennifer Daskal, "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge," Center for Strategic & International Studies, July 2018, 20, 14-16, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspiGYNGcGKTUjrGY3rN.

39 Peter Swire and DeBrae Kennedy-Mayo, "Why Both the EU and the US are "Stricter" than Each Other for the Privacy of Government Requests for Information," Emory Law Journal 66, no. 617 (2017), http://law.emory.edu/elj/_documents/volumes/66/3/swire-kennedy-mayo.pdf.

Along with these challenges to Indian law enforcement, this report highlights a broad range of existing mechanisms for cooperation and information-sharing on serious crimes. These current avenues exist between Indian law enforcement and US service providers as well as between the two governments. In addition, this report describes potential avenues under the recently passed US Cloud Act for Indian law enforcement to directly access to the stored the content of communications from US service providers.

The stakes are high if additional cooperation between India and the US is not possible to ensure Indian law enforcement timely access to the content of stored communications held by US service providers. Notably, arguments for data localisation[40] can become more persuasive if India lacks access to important evidence concerning serious crimes. As of the writing of this report, the Indian government is considering a bill that would require data localisation for most types of businesses; such a requirement is viewed as boosting law enforcement efforts to access information for crime prevention and for gathering evidence for prosecution.[41] Certain groups in India have asserted that data localisation is required to enable Indian law enforcement to access necessary evidence.[42] According to this point of view, data localisation would address concerns currently faced by law enforcement agencies in accessing evidence and sidestep the need to proceed through lengthy legal processes for cross-border transfers. Data localisation is also considered a means of exerting "data sovereignty," as opposed to having to comply with foreign legal requirements such as demonstrating "probable cause." In addition, data localisation has also been suggested as a way to prevent surveillance of Indian citizens' data by foreign states[43] and as a measure to boost home-grown businesses.[44] While there may be legitimate reasons to pursue data localisation, there have been significant concerns from various stakeholders, both inside and outside India, about unintended consequences. These potential consequences include stifling technological innovation, harming economic growth and creating difficulties for Indian start-ups looking to expand globally.[45] This paper highlights the possibility of an alternate approach, through a US - India Cloud Act Executive Agreement, that could help address some of the major concerns that have led to support for data localisation.

In this report, we suggest that solutions under the Cloud Act are more feasible than most people have realised. The US Cloud Act provides an avenue for countries to enter into an Executive Agreement with US which would allow these countries to deal directly with US service providers to access electronic evidence.

In this report, we suggest that solutions under the Cloud Act are more feasible than most people have realised.

40 A requirement that data be stored either exclusively on local servers or at least a copy of data be stored on local servers.

41 This requirement was proposed by an expert committee set up to draft a data protection law for India. Report on"A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 2017, 88, http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf ("Srikrishna Committee Report").

42 For eg., see Srikrishna Committee Report, 88; Dalip Singh, "Law enforcement agencies favour data localisation," The Economic Times, 8 October 2018, https://economictimes.indiatimes.com/news/economy/policy/law-enforcement-agencies-favour-data-localisation/articleshow/66113360.cms.

43 Srikrishna Committee report, 92.

44 Pratik Bhakta, "How local companies will gain from RBI's tough stance on data localisation," The Economic Times, 12 October 2018, https://tech.economictimes.indiatimes.com/news/startups/how-local-companies-will-gain-from-rbis-tough-stance-on-data-localization/66177688.

45 See Rahul Sachitanand, "All about India's data localisation policy," The Economic Times, 21 October 2018, https://economictimes.indiatimes.com/tech/ites/all-about-indias-data-localisation-policy/articleshow/66297596.cms; Regina Mihindukulasuriya, "Indian worker may lose 11% of monthly salary if data localisation becomes law, study says," The Print, 21 November2018, https://theprint.in/governance/indian-worker-may-lose-11-of-monthly-salary-if-data-localisation-becomes-law-study-says/152304/.

As part of the Executive Agreement, the foreign country must ensure adequate levels of criminal procedural protections for covered domestic crimes.[46]

Commentators on the Cloud Act have argued that an Executive Agreement between India and the US is impossible.[47] We disagree, and believe this report serves as a roadmap for how an Executive Agreement between India and the US could be carefully drafted to ensure that institutions and procedures are prudently crafted to meet the Cloud Act requirements to enable sharing of significant communications content.

In this report, we focus on two potential building blocks for an Executive Agreement between India and the US The first would involve designation of "sub-units" of the Indian government that could qualify to send requests directly to US service providers. Recognising that the sheer volume of all possible requests at all levels of the Indian government might significantly tax such a system, and the difficulty in training law enforcement at these various levels to comply with the complexities of US law on this subject, the designation of sub-units could allow for a manageable and auditable system for access to electronic evidence in cases of serious crimes. The second approach would build on existing procedures in Indian law. In the Executive Agreement between the two countries, the US could agree to allow direct access to US service providers only in instances when India agrees to use provisions of its own existing law that already provide a sufficient level of protection to individuals, such as the review of a request by an Indian judge.

Observer Research Foundation (ORF) and the Cross-Border Requests for Data Project of the Georgia Tech Institute for Information Security & Privacy have joined forces to write this report. ORF, in an earlier report,[48] examined the MLAT process and identified challenges faced by Indian law enforcement agencies in trying to access data through MLATs. Some of the key concerns highlighted were: lack of capacity within law enforcement in the generation and processing of data sharing requests; process delays; and differences in the treatment of data in India and the US. This research group at Georgia Tech has been examining the state of international MLA and other avenues for data sharing with various countries.[49] The research project headed by Peter Swire had, in 2015, proposed the idea that certain countries with high-quality procedures for seeking evidence could be eligible for a streamlined process for obtaining evidence in the US[50] This theoretical framework has been incorporated into the Cloud Act. In this report, the authors have collaborated to gather perspectives from both India and the US and provide a holistic view of India-US cooperation for law enforcement.

---

46 Executive Agreements under the US Cloud Act are discussed in Chapter VI of this report. For details regarding the requirements for an Executive Agreement, see Jennifer Daskal and Peter Swire, "Suggestions for Implementing the Cloud Act," Lawfare, 30 April 2018, https://www.lawfareblog.com/suggestions-implementing-cloud-act and Peter Swire and Jennifer Daskal, "What the cloud Act means for privacy pros," IAPP, 26 March 2018, https://iapp.org/news/a/what-the-cloud-act-means-for-privacy-pros/.

47 See Trisha Jalan, Report on panel discussion on "How does the Data Protection Bill deal with surveillance?," Medianama, 11 September 2018, https://www.medianama.com/2018/09/223-namaprivacy-how-does-the-data-protection-bill-deal-with-surveillance/.

48 Bedavyasa Mohanty and Madhulika Srikumar, "Hitting Refresh: Making India – US Data Sharing Work," ORF, August 2017, https://www.orfonline.org/wp-content/uploads/2017/08/MLAT-Book.pdf.

49 See Peter Swire and Justin Hemmings," Mutual Legal Assistance in an era of Globalized Communications: The Analogy to the Visa Waiver Program," NYU Annual Survey of American Law 71, no. 687 (2017), https://annualsurveyofamericanlaw.org/wp-content/uploads/2017/04/71-4_swirehemmings.pdf; "Stakeholders in Reform of the Global System for Mutual Legal Assistance," in Bulk Collection: Systemic Government Access to Private-Sector Data, eds. Fred H. Cate and James X. Dempsey (Oxford University Press, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2696163; Peter Swire, Justin D. Hemmings, and Suzanne Vergnolle, "A Mutual Legal Assistance Case Study: The United States and France," Wisconsin International Law Review 34, no. 323 (2017), http://hosted.law.wisc.edu/wordpress/wilj/files/2017/12/Final_Proof2.3.15.17.pdf; Peter Swire and DeBrae Kennedy-Mayo, "Why Both the EU and the US are "Stricter" than Each Other for the Privacy of Government Requests for Information," Emory Law Journal 66, no. 617 (2017), http://law.emory.edu/elj/_documents/volumes/66/3/swire-kennedy-mayo.pdf.

50 Peter Swire and Justin Hemmings, Mutual Legal Assistance in an era of Globalized Communications: The Analogy to the Visa Waiver Program," NYU Annual Survey of American Law 71, no. 687 (2017), https://annualsurveyofamericanlaw.org/wp-content/uploads/2017/04/71-4_swirehemmings.pdf; see also "Cross-Border Requests for Data Project" hosted by the Institute for Information Security & Privacy, http://www.iisp.gatech.edu/cross-border-data-project.

The report provides an overview of the two legal systems at issue, the existing types of cooperation and information sharing, and potential options for an Executive Agreement under the US Cloud Act. Chapter I of the report looks at the US and Indian legal systems. In each system, we examine general criminal procedure protections, specific procedures for electronic data, and repercussions for not complying with these legal requirements. Next, the report explores additional, often overlooked legal mechanisms for accessing electronic evidence and addressing Indian concerns about unlawful content. These include: methods currently available for cooperation and information sharing between India and US service providers and methods currently available for bilateral and multilateral cooperation and information sharing involving India and the US The report concludes by discussing in detail the possibility of an India/US Executive Agreement to streamline access to some communications content.

This project was envisioned to address the growing problem of Indian law enforcement's frustration with its ability to access to electronic evidence held by companies that are based outside of India. Our belief is that answers to this problem in India may be scalable to similar problems faced by other countries around the world.

This project was envisioned to address the growing problem of Indian law enforcement's frustration with its ability to access to electronic evidence held by companies that are based outside of India.

LAW AND PROCEDURE IN THE US FOR LAW ENFORCEMENT ACCESS TO STORED ELECTRONIC DATA

The US law presented in this section describes the legal protections that exist concerning law enforcement access to the content of stored communications held by US service providers; these protections exist to protect the person accused of a crime and more generally to safeguard society against the risk of abuse of police power. In this discussion, it is important to understand that these protections in US law, which restrain law enforcement, are the same whether the officer is from the US or from India. [51]

In a US criminal proceeding, the evidence obtained from a service provider cannot used be used if these protections are violated in accessing the evidence. The US doctrine known as the "exclusionary rule" bars evidence obtained in such an illegal search from being used at criminal trials.[52] A separate, but related, doctrine in US law has been termed the "the fruit of a poisonous tree," barring from criminal prosecutions any additional evidence derived from an illegal search.[53] These two doctrines provides significant protections against violation of criminal procedure requirements in US criminal cases.

Indian law, however, does not mirror these protections, i.e. evidence would be allowed in a criminal trial in India even if all legal requirements for obtaining the evidence were not precisely followed.[54] This difference raises a fundamental question for Indian law enforcement: why don't US service providers simply provide this evidence knowing that it is being used for a prosecution outside the US? The answer is straightforward: US service providers are concerned about the risk of civil and criminal sanctions if they release stored electronic communications in violation of US law.

Why don't US service providers simply provide this evidence knowing that it is being used for a prosecution outside the US? The answer is straightforward – US service providers are concerned about the risk of civil and criminal sanctions if they release stored electronic communications in violation of US law.

51 When a law enforcement agency from outside the US seeks data, it may send a request under a Mutual Legal Assistance Treaty (MLAT). The usual MLA process is as follows once the law enforcement request is sent to the US from the foreign country: (1) the DOJ reviews the request received from foreign law enforcement; (2) a US federal prosecutor appears before a US federal judge; and (3) the US prosecutor relays the law enforcement request from the requesting country, asking the judge to issue an order requiring production of the evidence. If the foreign law enforcement request does not contain sufficient details to allow the judge to make a finding concerning the requirements under US law, the requested evidence is likely to be delayed. Unless the foreign law enforcement officer adequately supplements the request, the evidence may not be received at all. See Chapter IV for a discussion on MLATs.

52 Mapp v. Ohio, 367 US 643, 657 (1961), https://www.law.cornell.edu/supremecourt/text/367/643. For details on the exclusionary rule, see Scott Sundby, "Everyman's Exclusionary Rule: The Exclusionary Rule and The Rule of Law (or Why Conservatives Should Embrace the Exclusionary Rule), Ohio State Journal of Criminal Law 10, no. 393, 2013, https://kb.osu.edu/bitstream/handle/1811/73400/OSJCL_V10N2_393.pdf). In addition to exclusion from evidence under the Fourth Amendment, certain statutes, such as the Wiretap Act, provide for exclusion of evidence for violation of the statutory requirements. See 18 U.S.C. § 2518(10)(a), https://www.law.cornell.edu/uscode/text/18/2518.

53 Wong Sun v. United States, 371 US 471, 487–88 (1963), https://caselaw.findlaw.com/us-supreme-court/371/471.html.

54 State of Maharashtra v. Natwarlal Damodardas Soni, AIR 1980 SC 593, https://indiankanoon.org/doc/6596/; Radhakrishnan v State of UP, 1963 Supp. 1 S.C.R. 408, https://indiankanoon.org/doc/1285567/.

Requests by Indian law enforcement officers would need to comply with US law to allow US service providers to release content of stored electronic communications under the current formal mechanisms discussed in Chapter IV. A short primer on relevant US law is provided here, first looking at the protections under the US Constitution: the requirement for a judge-issued warrant detailing the location to be searched and the items to be seized and finding "probable cause" that a crime has occurred and that contraband or evidence of the crime will be found by the search. The US concept of "probable cause" is discussed in some detail, as it is likely unfamiliar to Indian readers. We next examine the current interpretation of the Electronic Communications Privacy Act (ECPA) which requires law enforcement to comply with US statutory standards to access stored electronic communications. This Chapter concluded with a discussion on the civil and criminal penalties that service providers can face if they violate the requirements of ECPA.

A. The Fourth Amendment to US Constitutional requires that law enforcement obtain a properly issued search warrant prior to conducting the search

The US Constitution requires protections against the potential for law enforcement overreach that must be met prior to a judge authorising a request for the collection of evidence for a criminal case.[55] The Fourth Amendment of the US Constitution provides the baseline rule that prohibits an officer of the government from conducting "unreasonable searches or seizures." In practice, the Fourth Amendment sets the default rule that any "search" or "seizure" without a warrant is deemed to be unreasonable; a warrant is obtainable by a law enforcement request to a judge only after the identification of the specific place to be searched and items to be seized as well as a finding that the key American standard of "probable cause" has been met.[56]

The primary source of these protections is the Fourth Amendment to the US Constitution:

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 an Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.[57]

The text of the Fourth Amendment is the source of three key protections found in US law including: 1) law enforcement must obtain approval from an independent judicial officer prior to conducting a search; 2) for a search warrant to be issued, the judge must find that the law enforcement request identified, with particularity, the place to be searched and the items to be seized; and 3) for a search warrant to be issued, the judge must find that the law enforcement request established "probable cause."

1. For a lawful search to be conducted, law enforcement must obtain a search warrant from a judge prior to conducting the search

In the US search warrants in criminal cases are issued by a judge.

In the US, search warrants in criminal cases are issued by a judge.[58] The judiciary in the US

55 These protections are designed into the US system from its founding, as a response to the abuses of government suffered by American colonists in the 18th Century. The Bill of Rights to the United States Constitution, comprised of the first ten amendments to the US Constitution, was adopted in 1791. The amendment primarily discussed in this section, the Fourth Amendment, has been in place since that time. See Bill of Rights, The National Constitution Center, https://constitutioncenter.org/learn/educational-resources/historical-documents/bill-of-rights.

56 US service providers may provide the content of communication to law enforcement under emergency situations, where the provider reasonably believes there is an "emergency involving danger of death or serious physical injury to any person." 18 U.S.C. 2702(b)(8), https://www.law.cornell.edu/uscode/text/18/2702.

57 US CONST. amend. IV. "Government" in this context means any person acting on behalf of a federal or state entity.

58 This review by an independent judge, separate from the executive branch, is far from universal in legal systems around the world. Even in the United Kingdom, which shares a common law history with the United States, the independent judiciary plays a far smaller role in overseeing criminal investigations than in the United States. See Regulation of Investigatory Powers Act 2000, § 5 (Eng.), https://www.legislation.gov.uk/ukpga/2000/23/contents; see also Peter Swire and DeBrae Kennedy-Mayo, "Why Both the EU and the US are 'Stricter' than Each Other for the Privacy of Government Requests for Information," Emory Law Journal 66, no. 617 (2017), http://law.emory.edu/elj/_documents/volumes/66/3/swire-kennedy-mayo.pdf.

is a separate branch of government, established by Article III of the US Constitution.[59] Federal judges are nominated by the President and confirmed by the Senate.[60] The independence of federal judges is provided in the Constitution—appointments are for the lifetime of the judge, with removal only by impeachment, and with a guarantee of no diminution of salary.[61]

When a judge receives a request from law enforcement to obtain evidence, the judge reviews that request to determine whether the protections required by the Fourth Amendment to the US Constitution have been met. As part of the independent assessment, the judge looks at whether the request provides specific details about the location to be searched and the items to be seized. Next, the judge assesses whether the law enforcement request has met the US standard to justify the search by law enforcement, meaning whether there is "probable cause" to believe that a crime has occurred.

2. For a search warrant to be issued, the judge must find that the law enforcement request identified, with particularity, the place to be searched and the items to be seized

One of the elements that must be present for a search warrant to be issued is a finding by a judge that the law enforcement request detailed, with particularity, the place to be searched and the items to be seized.[62] General warrants, which would authorise the law enforcement officer to make a general search of places of interest for numerous types of items, are strongly disfavoured in the US legal tradition.[63] The requirement in US law limits the scope of the search by law enforcement, both as to place searched and items seized. The restrictions require that the law enforcement request provide particular details of the location to be searched as well as the items to be seized during the search. With this information provided in the law enforcement request, the judge is able to make a determination as to whether the requested search is sufficiently linked to the alleged crime and to ensure that eventual search and seizure is limited.[64]

3. For a search warrant to be issued, the judge must find that the law enforcement request established "probable cause"

Along with particularity of the search, "probable cause" must be established for a judge to issue a search warrant.[65] In the research conducted at Georgia Tech on MLA, we have found that the probable cause standard is different than the legal rules in other countries, and is generally considered stricter than non-US practice before the government

Realising that the "probable cause" standard is likely unfamiliar to Indian law enforcement, this section discusses the standard in some detail.

59 US CONST. art. III, § 1, https://www.law.cornell.edu/constitution/articleiii.

60 US CONST. art. II, § 2, https://www.law.cornell.edu/constitution/articleii.

61 US CONST. art. III, § 1, https://www.law.cornell.edu/constitution/articleiii.

62 Annotation 2 – Fourth Amendment, Find Law for Legal Professionals, https://constitution.findlaw.com/amendment4/annotation02.html#t89; see Particularity, Justia US Law, https://www.justia.com/criminal/docs/search-seizure-faq/#q3 .

63 Prior to the founding of United States when the territory was a colony of Great Britain, the British Government issued general warrants that allowed the law enforcement officer in possession of the warrant to search for any item believed to be in the colonies illegally, without specifying either where the item was located or the specific item sought. Encyclopedia Britannica, Writ of Assistance, https://www.britannica.com/topic/writ-of-assistance.

64 Annotation 2 – Fourth Amendment, Find Law for Legal Professionals, https://constitution.findlaw.com/amendment4/annotation02.html#t89

65 Lesser standards apply in certain situations that are not covered by the Fourth Amendment. See Peter Swire and DeBrae Kennedy-Mayo, "Why Both the EU and the US are 'Stricter' than Each Other for the Privacy of Government Requests for Information," Emory Law Journal 66, no. 617 (2017), http://law.emory.edu/elj/_documents/volumes/66/3/swire-kennedy-mayo.pdf. For a discussion of requests by Indian law enforcement for certain types of non-content data, see Chapter V.A.1.

can access evidence.[66] Since the "probable cause" standard is likely unfamiliar to Indian law enforcement, this section discusses the standard in some detail.

Probable cause is not clearly defined in the US Constitution. Consequently, the US Supreme Court has attempted to clarify the term on several occasions,[67] but has generally favoured a flexible approach, viewing probable cause as a "practical, non-technical" standard that examines the "factual and practical considerations of everyday life."[68]

In defining the "probable cause" standard, the US Supreme Court has determined that warrants should only be issued by a judge when, according to "all the circumstances" presented by the requesting party, "there is a fair probability that contraband or evidence of a crime will be found in a particular place."[69] In Illinois v. Gates, the Court wrote that "probable cause is a fluid concept–turning on the assessment of probabilities in particular factual context–not readily, or even usefully, reduced to a neat set of legal rules."[70]

The following cases provide insight on how the strict requirements of the Fourth Amendment—a judge-issued warrant based upon probable cause—apply to changing technology:

a. Katz v. United States (reasonable expectation of privacy):[71] The 1967 Katz case created the rule that a warrantless search is "unreasonable" when there is both an actual individual expectation of privacy in the relevant evidence and a socially accepted expectation of privacy in that evidence. In this seminal case, a suspect was calling in gambling information on a public phone booth; the police performed a wiretap without a warrant to access these phone calls.[72] The Court held that "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[73] Since adopting this two-pronged test for reasonableness, the Court has re-examined these parameters in the face of changing technology.

b. Kyllo v. United States (search of house conducted from the street):[74] In this 2001 case, the Court grappled with the concept of whether law enforcement should be able to surveil activity within a house via technology, when the officers remained physically outside the home. In the Kyllo case, the police tried to rely on a longstanding doctrine that permitted the police to gather evidence that is in "plain view" to use a thermal imaging device to detect a high level of electricity in a house. These levels of use are often associated with growing marijuana. The Court stated, "Where, as here, the Government uses a device that is not in general use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is

---

66 Peter Swire and DeBrae Kennedy-Mayo, "Why Both the EU and the US are 'Stricter' than Each Other for the Privacy of Government Requests for Information," Emory Law Journal 66, no. 617, 643 (2017), http://law.emory.edu/elj/_documents/volumes/66/3/swire-kennedy-mayo.pdf.

67 See, e.g., Maryland v. Pringle, 540 US 366, 370–71 (2003), https://www.supremecourt.gov/opinions/03pdf/02-809.pdf; Gerstein v. Pugh, 420 US 103, 111 (1975), https://caselaw.findlaw.com/us-supreme-court/420/103.html; Carroll v. United States, 267 US 132, 161–62 (1925), https://caselaw.findlaw.com/us-supreme-court/267/132.html.

68 See Illinois v. Gates, 462 US 213, 231 (1983) (citing Brinegar v. United States, 338 US 160, 176 (1949)), https://caselaw.findlaw.com/us-supreme-court/462/213.html.

69 See Illinois v. Gates, 462 US 213, 238 (1983). The probable cause standard is different than the legal rules in other countries, and generally considered stricter than non-US practice before the government can access evidence. Peter Swire and DeBrae Kennedy-Mayo, "Why Both the EU and the US are 'Stricter' than Each Other for the Privacy of Government Requests for Information," Emory Law Journal 66, no. 617 (2017), http://law.emory.edu/elj/_documents/volumes/66/3/swire-kennedy-mayo.pdf; see Peter Swire, Justin Hemmings and Suzanne Vergnolle, "A Mutual Legal Assistance Case Study: The United States and France" Wisconsin International Law Journal 34, no. 323 (2017), http://hosted.law.wisc.edu/wordpress/wilj/files/2017/12/Final_Proof2.3.15.17.pdf.

70 Id. at 232.

71 389 U. S. 347, 353 (1967), https://www.law.cornell.edu/supremecourt/text/389/347. The enduring test from Katz, however, comes from Justice Harlan's concurrence where he wrote that the Fourth Amendment protects people through "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognise as 'reasonable.'" Katz at 361 (J. Harlan, concurring).

72 Katz, 389 U. S. 347 (1967), https://www.law.cornell.edu/supremecourt/text/389/347.

73 Katz at 358 (1967), , https://www.law.cornell.edu/supremecourt/text/389/347.

74 Kyllo v. United States, 533 US 27 (2001), https://www.law.cornell.edu/supct/html/99-8508.ZO.html.

a 'search' and is presumptively unreasonable without a warrant." This holding constrained police surveillance even when the evidence was gathered from the public street without entering the home.

c. United States v. Jones (search conducted in public):[75] In 2012, the Court examined the use of an electronic tracking device placed onto a vehicle. The longstanding rule had been that police can "tail" a suspect in public, meaning that the officers can follow people in public places. In the Jones case, police had placed tracking devices on objects. (The Supreme Court had previously ruled that the tracking device could not enter the home without a warrant but had never prohibited tracking a suspect in public). In this case, the Court unanimously held that a warrant was required for a tracking device to be put on a suspect's car for 30 days. One problem the Court identified was that the police were "trespassing" on the suspect's car when they attached a device. Justices wrote at length about the constitutional protections necessary to prevent long-term and widespread surveillance in public, in light of changing technology.

d. Riley v. California (cell phones):[76] In 2014, the Court considered the appropriate protections regarding the data stored on a cell phone. The longstanding rule has been that police can search a person "incident to arrest," meaning they could go through the person's pockets to spot possible weapons or evidence. In the Riley case, the government took the position that this rule applied to cell phones, but the Supreme Court unanimously disagreed. The Court held that a judicial warrant was needed before the police could search the contents of the cell phone. The Court said, "a cell phone search would typically expose to the government far more than the most exhaustive search of a house." In short, the Court updated fundamental rights protections to adapt to the changing technology of the cell phone.

e. Carpenter v. United States (cell-site location information):[77] In 2018, the United Supreme Court reigned in the application of the "third-party" doctrine,—the concept that a person does not have a reasonable expectation of privacy in records held by a third party, including bank records and pen registers,[78] and that therefore a warrant is not required for these records.[79] Finding that cell-site location information could reveal intimate details about the habits of individuals' lives and that the cell phone usage was integral to modern life, the Court held that law enforcement must secure a warrant to access these records

---

75 United States v. Jones, 132 S. Ct. 945 (2012), https://www.supremecourt.gov/opinions/11pdf/10-1259.pdf.

76 Riley v. California, 134 S. Ct. 2473 (2014), https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

77 Carpenter v. United States, United States Supreme Court decision, No.16-402, June 2018, https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf. See Kimberly Kiefer Peretti, Lawrence R. Sommerfeld and Nameir Abbas, "US Supreme Court Builds On Individuals' Privacy Rights," Alston & Bird, 26 July 2018, https://www.alston.com/en/insights/publications/2018/07/us-supreme-court-builds-on-individuals-privacy (for an analysis of the Carpenter ruling).

78 "Pen registers" are records of dialed phone numbers. In Carpenter, the records at issue had been acquired under the ECPA's requirement for "specific and articulable facts." The Court determined this was not sufficient protection for the cell-location data.

79 The third party doctrine, which states there is no reasonable expectation of privacy in information shared with a third party business, arises from US Supreme Court cases including Miller and Smith. In US v. Miller, 425 US 435 (1976), https://caselaw.findlaw.com/us-supreme-court/425/435.html, the Court held that a defendant had no reasonable expectation of privacy in the bank records associated with revenue he earned through making bootleg liquor with an unregistered still and on which he did not pay taxes. Miller at 436. The Court pointed to Katz's language stating that "[w]hat a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection." Miller at 442 (citing Katz). The Court in Miller noted that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." Miller at 443. The same principle was applied in Smith v. Maryland, 442 US 735 (1935), https://caselaw.findlaw.com/us-supreme-court/442/735.html, where the Court held that a pen register was covered under the third party doctrine. Smith at 743-44. The Court reasoned that "[w]hen he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, the petitioner assumed the risk that the company would reveal to police the numbers he dialed." Smith at 744. Peter Swire, Justin Hemmings, and Suzanne Vergnolle, "A Mutual Legal Assistance Case Study: The United States and France," Wisconsin International Law Review 34, no. 323 (2017), http://hosted.law.wisc.edu/wordpress/wilj/files/2017/12/Final_Proof2.3.15.17.pdf; but see Orin Kerr, The Case for the Third-Party Doctrine, 107 Mich. L. Rev. 561, 2009, https://repository.law.umich.edu/mlr/vol107/iss4/1 (on ongoing usefulness of the third party doctrine).

In summary, these US Supreme Court cases have shown that the relatively strict protections of the Fourth Amendment—a probable cause warrant with particularity—are likely to be extended to new technologies that reveal intimate information about a person's life. In addition to these Supreme Court cases, the widely influential 6th Circuit case of United States v. Warshak[80] interpreted ECPA to say that requests for the content of communications, such as e-mails, require a judge-issued search warrant based on "probable cause."[81] Because of US Supreme Court's history of applying strict Fourth Amendment protections to changing technologies, observers have expressed their belief that there is a strong likelihood the Warshak approach would be adopted if the US Supreme Court were to review this topic.[82]

These US Supreme Court cases have shown that the relatively strict protections of the Fourth Amendment – a probable cause warrant with particularity – are likely to be extended to new technologies that reveal intimate information about a person's life.

B. Current practice in the US is to interpret the Electronic Communications Privacy Act (ECPA) to require law enforcement to comply with the protections of the Fourth Amendment to the US Constitution to access stored electronic communications

Under ECPA, service providers are prohibited from disclosing communications content to any government entity, US or non-US.[83] An exception to this prohibition is when a US government entity requires disclosure of content using appropriate legal process (described later in this section). This is the channel under ECPA which enables non-US governments to make requests for content through the MLAT process – using US legal process for making requests through the US government. The Cloud Act provides a new exception for non-US governments to seek content from service providers. Where an Executive Agreement under the Cloud Act is in place between US and another government, the non-US government can gain access to content from a US service provider pursuant to such agreement. Importantly, there is no similar prohibition on a service provider giving access to subscriber and metadata to the foreign government. The strict prohibition against sharing with non-US governments applies only with content.[84]

Here, we describe the US legal process for accessing content under ECPA. Based on current interpretations of ECPA, law enforcement requests for access to stored electronic communications held by US service providers must meet the requirements of the Fourth Amendment to the US Constitution – most importantly, search and seizure of the contents of stored electronic communications can only be conducted after a judge has made a decision to issue a warrant based on probable cause. This current interpretation is based on decisions by federal court judges that was then adopted as standard practice by the US Department of Justice (DOJ).

---

80 United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010), http://www.opn.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf (holding the Fourth Amendment prevents law enforcement from obtaining stored e-mail communications without a warrant based on probable cause); see also United States v. Ali, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012), ("[I]ndividuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial internet service provider." (quoting United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011))).

81 Orin Kerr, "Does Carpenter Revolutionize the Law of Subpoenas?" Lawfare, 26 June 2018, https://www.lawfareblog.com/does-carpenter-revolutionize-law-subpoenas.

82 After Warshak, the DOJ updated its practice when seizing stored electronic communications to require law enforcement to require for its own prosecutions a judge-issued warrant in compliance with the protections of the Fourth Amendment to the US Constitution. ECPA (Part I): Lawful Access to Stored Content: Hearing before the Subcommittee on Crime, Terrorism, Homeland Sec., and Investigations of the Comm. of the Comm. on the Judiciary, H.R., 113th Cong. 14 (2013) (statement of Elana Tyrangiel, Acting Assistant Att'y Gen., Office of Legal Policy, Department of Justice), https://judiciary.house.gov/_files/hearings/printers/113th/113-16_80065.PDF.

83 18 U.S.C. 2702(a)(1) and (2), https://www.law.cornell.edu/uscode/text/18/2702.

84 See Chapter V.A.1 for a discussion on the channel through which Indian law enforcement could directly seek certain non-content data from US service providers.

The text of ECPA has complex requirements for disclosures made by service providers in response to law enforcement requests.[85] Relevant to this discussion are the legal protections that must be satisfied for a service provider to release the content of stored electronic communications. After the Warshak case discussed in subsection (A), the DOJ updated its practice when seizing stored electronic communications to require law enforcement to obtain a judge-issued warrant in compliance with the protections of the Fourth Amendment to the US Constitution.[86]

C. US service providers who release electronic evidence in violation of ECPA risk civil and criminal penalties for their actions

In interviews with US service providers, we have learned that companies have significant concerns about their own risk of civil and criminal penalties if the access that they provide to law enforcement does not comply with the protections of ECPA and the US Constitution.

ECPA provides for two criminal charges. Under the first provision for criminal penalties, an individual who unlawfully accesses stored electronic communications or exceeds an authorisation permitting access for listed purposes, is subject to a criminal fine, up to five years imprisonment, or both for a first offence.[87] A first offence carries a penalty of criminal fine and/or imprisonment up to one year, and subsequent offences carry a penalty of criminal fine and/or imprisonment up to five years.[88] In certain instances, the penalty increases to criminal fines, up to ten years imprisonment, or both.[89]

The second provision of ECPA provides for criminal penalties when an individual unlawfully accesses stored electronic communications or exceeds an authorisation permitting access "in any other case" (than the reasons mentioned in the first criminal provision) is subject to a fine, imprisonment not to exceed one year, or both, for the first offence. Any subsequent conviction results a fine, up to five years imprisonment, or both.[90]

In addition to the criminal penalties for violations of ECPA, the statute includes civil penalties for inappropriate disclosure. Individuals whose stored electronic communication was released in violation of the law have the right to bring a civil suit against the company seeking monetary compensation (up to USD 1,000) and reasonable attorneys' fees.[91]

In summary, the US legal system provides for constitutional protections for the collection of evidence by law enforcement. The Fourth Amendment to the US Constitution requires a judge-issued warrant that particularly describes the place to be searched and items to be seized as well as a finding of probable cause. The US Supreme Court has determined that these Fourth Amendment protections extend to many new technologies. According to the lower court ruling in Warshak, ECPA requires this strict level of protection for law enforcement to access the content of stored electronic communications. The holding in Warshak has been adopted both the DOJ

---

85 See § 201, 100 Stat. at 1860 (codified as amended at 18 U.S.C. §§ 2701-10) (enacted as Title II of ECPA); § 201, 100 Stat. at 1861.

86 Lawful Access to Stored Content: Hearing before the Subcommittee on Crime, Terrorism, Homeland Sec., and Investigations of the Comm. of the Committee on the Judiciary, H.R., 113th Cong. 14 (2013) (statement of Elana Tyrangiel, Acting Assistant Att'y Gen., Office of Legal Policy, Department of Justice), https://judiciary.house.gov/_files/hearings/printers/113th/113-16_80065.PDF. For an overview of company policies that adopt Warshak's requirement for a search warrant based on probable cause, see Liz Woolery, Ryan Budish, and Kevin Bankston, Memo 4: Reporting on the Legal Processes Required for User Information, Survey and Best Practices Memos, The Transparency Reporting Toolkit, p. 51-60, https://cyber.harvard.edu/sites/cyber.harvard.edu/files/Final_Transparency.pdf.

87 These listed purposes are "commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act." 18 U.S.C. § 2701(b)(1)(A); see Congressional Research Service, Privacy: An Overview of the Electronic Communications Privacy Act, p. 35, 45; https://fas.org/sgp/crs/intel/98-326.pdf. Because the Stored Communications Act (SCA) is part of ECPA, only the term ECPA is used in this report. See Congressional Research Service, Privacy: An Overview of the Electronic Communications Privacy Act, p. 35, https://fas.org/sgp/crs/intel/98-326.pdf.

88 18 U.S.C. § 2701(b)(2), https://www.law.cornell.edu/uscode/text/18/2701.

89 Id. § 2701(b)(1)(B), https://www.law.cornell.edu/uscode/text/18/2701.

90 18 U.S.C. § 2701(b)(2), https://www.law.cornell.edu/uscode/text/18/2701.

91 18 U.S.C. 2707, https://www.law.cornell.edu/uscode/text/18/2707; see Congressional Research Service, "Privacy: An Overview of the Electronic Communications Privacy Act," 45, https://fas.org/sgp/crs/intel/98-326.pdf.

in its internal requirements for prosecutions and by many service providers in their approach to responding to law enforcement requests for evidence. Service providers must be particularly careful in responding to requests for the content of stored electronic communications as they face civil and criminal penalties if they violate ECPA.

LAW AND PROCEDURE IN INDIA FOR LAW ENFORCEMENT ACCESS TO STORED ELECTRONIC EVIDENCE

For successful requests for access to the content of stored electronic communications, Indian law enforcement will need to fulfil the requirements under US law as well as Indian law. In this chapter, we examine Indian laws to highlight both similarities and distinctions between the two legal systems.

There are overarching protections relating to privacy flowing from the Indian Constitution and some of these protections relate to protection against surveillance by law enforcement.

Prior to starting our in-depth look at relevant Indian law, it is important to discuss certain key points relating to Indian constitutional and statutory law on the subject. First, there are overarching protections relating to privacy flowing from the Indian Constitution[92] and some of these protections relate to protection against surveillance by law enforcement.[93] The jurisprudence relating to law enforcement and privacy, however, has evolved in a different way than in the US One of the key differences is that, unlike US constitutional law, there has been no general requirement in India for judicial authorisation for accessing stored communications content.[94] Constitutional law in this field is still evolving, however, and use of new technologies and tools by government and law enforcement could be open to judicial scrutiny.[95]

Second, unlike US law where there is a clear distinction between real-time interception and access to stored content, the protections in the IT Act related to interception are ambiguous and could arguably be read to cover both access to stored content and real-time interception.[96]

---

92 Although not expressly mentioned in the Constitution, the right to privacy has been understood as emanating from other constitutionally guaranteed fundamental rights, such as the right to life and personal liberty (Article 21 of the Indian Constitution), the right to freedom of movement (Article 19(1)(d)), and the freedom of speech and expression (Article 19(1)(a)), among others.

93 See, for eg., Kharak Singh v. State of Uttar Pradesh, 1964 SCR (1) 332, https://indiankanoon.org/doc/619152/, where the Supreme Court struck down state regulations that authorised police officers to make visits at night to a suspect's home. (The majority opinion, in this case, however did not hold privacy to be a constitutionally protected right, and to that extent the ruling has been overruled by K.S. Puttuswamy v. Union of India, 2017 (10) SCALE 1, https://indiankanoon.org/doc/91938676/). More recently, in a challenge to Aadhaar, India's biometric identity project, a provision enabling disclosure of certain information through a direction by a Joint Secretary was struck down noting that a higher ranking authority or a judicial officer should authorise such disclosure. Puttuswamy v. Union of India, 2018, https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf.

94 In People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301, https://indiankanoon.org/doc/31276692/, the Supreme Court declined to impose the requirement of prior judicial scrutiny for telephone tapping orders but did lay down other procedural safeguards, such as issuance of orders by certain senior government officers and review by a separate committee.

95 A recent example is the challenge to the Aadhaar project – which provides a biometric identity based service delivery platform. See Justice Puttaswamy v. Union of India and Others, Supreme Court of India, 2018, https://indianexpress.com/article/india/aadhaar-verdict-full-text-judgment-supreme-court-order-5374794/; see also "Supreme Court Gives Aadhaar Some Privacy," The Indian Express, 27 September 2018, https://indianexpress.com/article/india/supreme-court-aadhaar-verdict-some-right-to-privacy-5376298/

96 The provision for accessing data refers to interception, monitoring, or decryption of "any information through any computer resource." Intercept as defined in the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 (https://indiankanoon.org/doc/30809273/) includes "viewing, examination or inspection of the contents of any direct or indirect information" and the IT Act itself requires intermediaries to extend assistance in providing information stored in a computer.

With regards to the particulars of this Chapter, we examine two categories of applicable India law: a) general criminal procedure law found in the Criminal Procedure Code 1973 CrPC;[97] and b) special protections for electronic evidence found in the Information Technology Act 2000 (IT Act).[98]

A. General criminal procedural law in Indian law for obtaining evidence for criminal cases

Under Indian law, the general criminal procedural law that relates to law enforcement access to evidence is found in the CrPC. The provisions of the Code relevant to this discussion are Section 91 and Section 93.

1. Under Section 91, Indian law enforcement has two avenues to require production of documents – one by law enforcement and a second by a judge

Section 91 of the CrPC provides two paths for law enforcement to seek evidence: any police officer in charge of a police station or any judge can compel the production of any "document or other thing" that is necessary or desirable for the purposes of an investigation or trial.

Section 91 of the CrPC provides two paths for law enforcement to seek evidence: any police officer in charge of a police station or any judge can compel the production of any "document or other thing" that is necessary or desirable for the purposes of an investigation or trial.[99]

The first path, under Section 91, is typically used by law enforcement without seeking judicial approval.[100] In this approach, the police officer issues a written order to the person who is in possession of the document or thing, requiring the person to produce it at the time and place stated in the written order.

Section 91 authorises a second path: a court may issue summons to require the production of documents.[101] This alternative summons route is not routinely used by law enforcement for accessing data. More typically, this route has been used by the prosecution, by the accused persons, and by complainants to approach courts to direct production of certain documents.

Practically speaking, when law enforcement seek production during an investigation, they most often issue a written order directly, and when a person other than the investigating authority seeks production when the case is at trial, they approach the court.[102] Section 91 appears to

97 The Code of Criminal Procedure, 1973 ("CrPC"), https://indiankanoon.org/doc/445276/.

98 The Information Technology Act, 2000, ("IT Act") https://indiankanoon.org/doc/1965344/.

99 These requirements have generally been interpreted broadly, requiring only relevance to an investigation. See Neelesh Jain v. State of Rajasthan 2006 CriLJ 2151 (Rajasthan HC), https://indiankanoon.org/doc/1135280/ ("The power given under section 91 of the code is a general and wide power which empowers the court, the production of any document or any other thing at any stage of any investigation, inquiry or other proceedings under the Cr.P.C. ... It is no doubt true that such power would not be exercised where the documents or thing may not be found relevant or it may be for the mere purpose or delaying the proceedings or the order is sought with an oblique motive."); Alagesan and Others v. State (2008) Cri.L.J. 3300 (Madras), https://indiankanoon.org/doc/626855/.

100 For Indian law enforcement who may be accustomed to having approval of search warrants either by law enforcement officials or by a judge, it is important to note that this requirement in US law for approval by an independent judicial officer cannot be met when the person issuing the warrant is engaged in law enforcement activities. See Annotation 2 – Fourth Amendment, Find Law for Legal Professionals, https://constitution.findlaw.com/amendment4/annotation02.html#t89

101 Summons may also be issued by courts to require appearance of a person.

102 Note that the procedure for seeking documents in civil proceedings are different and are set out in the Civil Procedure Code.

enable a law enforcement agency to approach a court for issuance of summons for compelling production of a document at any stage of a criminal proceeding, although in practice law enforcement generally issue a written order for easy access during an investigation.[103]

2. Under Section 93, Indian law enforcement can obtain a search warrant from a judge

Section 93 of the CrPC sets out three situations where search warrants can be issued by judges.

Section 93 of the CrPC sets out three situations where search warrants can be issued by judges. First, if a court has reason to believe that a person to whom a summons or order has been addressed will not produce the specific document requested pursuant to a Section 91 demand, the court can issue a search warrant, which directs a person (typically law enforcement) to carry out a search or inspection.[104] From a reading of the provision, it appears that a search warrant can be sought where the person possessing the document will not voluntarily furnish it. This could create a conflict for a US service provider that is required to produce a document by an Indian court while at the same time, is not allowed to disclose content under applicable US law.

The other two scenarios where a court can issue a search warrants are either where a document is not known to the court to be in the possession of any person,[105] or where the court considers that an inquiry, trial, or other proceeding will be served by a general search or inspection.[106] This portion of Section 93 indicates that general searches can be directed through search warrants.

Importantly, in all three scenarios, the court can, in its discretion, specify the place where the warrant is to extend.[107] Thus, although this is not a mandatory requirement, courts retain the legal authority to set forth specificity in warrants. This portion of the provision does not set out other requirements or limitations for search warrants.[108]

B. Statutory protections in Indian law relevant to Indian law enforcement accessing electronic evidence under the Information Technology Act (IT Act)

In Indian law, the procedures specific to electronic evidence are found in the Information Technology Act (IT Act).[109] The IT Act is the primary law in India governing electronic commerce and cyber crime, and has specific provisions on interception of electronic communications, different from the procedures set out in the CrPC for getting evidence. It should be noted that the IT Act has an overriding clause stating that its provisions would have effect over anything inconsistent in other laws in force at the time.[110] Given that this is a special statute and has a specific provision to that effect, to the extent there are special procedures in the law for obtaining access to electronic information, those are likely to prevail over general procedures set out in the

---

103 The Supreme Court has observed that a police officer could move the court for summoning and production of a document at any stage mentioned in Section 91, which includes investigation. See State of Orissa vs. Debendra N. Padhi (2005) 1 SCC 568, https://indiankanoon.org/doc/7496/ ("When the section refers to investigation, inquiry, trial or other proceedings, it is to be borne in mind that under the section a police officer may move the Court for summoning and production of a document as may be necessary at any of the stages mentioned in the section.")

104 CrPC, S.93(1)(a) , https://indiankanoon.org/doc/983956/. Case law on the provision has largely been about whether this provision can be invoked to direct accused persons to produce incriminating documents. V.S.Kuttan Pillai v. Ramakrishnan and another AIR 1980 SC 185, https://indiankanoon.org/doc/68260/.

105 CrPC, S.93(1)(b), https://indiankanoon.org/doc/983956/.

106 CrPC, S.93(1)(c) , https://indiankanoon.org/doc/983956/.

107 CrPC, S.93(2) , https://indiankanoon.org/doc/983956/.

108 CrPC, S93(1)(c). See Chapter VI, Section C for a discussion on the significance of the ability of the courts to issue specific rather than general warrants.

109 In addition, the Telegraph Act (and specifically Telegraph Rules) also specify procedures for interception of communication that are similar to the IT Act procedures. This regime governs telecommunication service providers that are licensees under the Telegraph Act.

110 IT Act, S.81, https://indiankanoon.org/doc/1932336/.

CrPC.[111] The IT Act does have special procedures for "interception, monitoring and decryption." It is not entirely clear whether interception here includes both real-time interception and access to stored communication. If the IT Act intends to cover only real-time interception, the CrPC provisions could still be said to prevail for accessing stored content. If the IT Act intends to cover both, the IT Act provision would occupy the field for stored content as well. From our interviews, it appears that police officers have continued to make requests for stored content pursuant to the CrPC, despite the IT Act provisions.

Under the IT Act, an authorised officer[112] of the central or state government can direct an agency of the appropriate government, apparently including law enforcement agencies, to intercept or monitor communications in real time or decrypt stored data.[113] Such direction can be issued if it is necessary for certain aims, such as protecting sovereignty or integrity of India, defence of India, security of the State, public order, or for investigation of any offence.[114]

Interception is subject to certain safeguards that are prescribed by rules made for this purpose.[115] According to these rules, interception can only be carried out under a direction issued by the "competent authority."[116] The competent authority designated for this purpose is the Secretary, Ministry of Home Affairs where it concerns the Central Government, or the Secretary, Home Department, in case of a state government or Union Territory.[117] Certain security and intelligence agencies have been authorised to carry out the interception or monitoring – these include the Central Bureau of Investigation, the Intelligence Bureau and the National Investigation Agency.[118] The rules also provide that in "unavoidable circumstances," the direction may be issued by a Joint Secretary of the central government (or a higher-ranked officer) who has been authorised by the competent authority. The IT Interception rules have some safeguards for the interception direction, namely, the competent authority should issue a direction only when it is not possible to acquire the information through other reasonable means,[119] the direction should specify the officer to whom the information will be disclosed,[120] and the direction will be in force for 60 days

111 We understand from interviews with stakeholders in India that law enforcement have continued to rely on the general procedures under the CrPC for making requests.

112 Any officer can be authorised to issue orders for this purpose. Under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 (https://indiankanoon.org/doc/30809273/), the Secretary in the Ministry of Home Affairs (for the central government) and the Secretary in the Home Department (for state governments) have been designated as 'competent authorities' who can issue orders for interception, monitoring or decryption.

113 IT Act, S.69, https://indiankanoon.org/doc/1439440/. The IT Act separately provides for the collection of "traffic data," which appears to include basic subscriber information (BSI). Traffic data is defined as "any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data, size, duration or type of underlying service or any other information." The procedure for monitoring and collecting traffic data is similar to that for interception of communication in some respects, for instance, like interception, monitoring or collection of traffic data can only be carried out through a direction issued by a competent authority (a government officer of a certain rank). Unlike interception though, collection of traffic data can be done for a broad range of purposes related to cyber security, including forecasting of cyber incidents, identification of viruses, and tracking breaches. See IT Act, S.69B, https://indiankanoon.org/doc/100506284/ and the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009, https://indiankanoon.org/doc/180294833/. In US law, the protections for accessing BSI are fairly minimal (typically through a subpoena) while for the content of communications, a warrant is required (a strong protection). In contrast, the legal instrument for getting access to both BSI and content in Indian law is a direction by a competent authority (although accessing BSI is subject to fewer safeguards).

114 IT Act, S.69, https://indiankanoon.org/doc/1439440/.

115 The Information Technology (Procedures for Interception or Monitoring or Decryption of Information) Rules 2009, https://indiankanoon.org/doc/30809273/ ("IT Interception Rules").

116 IT Interception Rules, R.3, https://indiankanoon.org/doc/30809273/.

117 IT Interception Rules, R.3, https://indiankanoon.org/doc/30809273/.

118 Ministry of Home Affairs order dated 20 December 2018, https://www.bloombergquint.com/politics/government-allows-10-central-agencies-to-monitor-decrypt-any-computer-data#gs.hq_NFz4.

119 IT Interception Rules, R.8, https://indiankanoon.org/doc/30809273/.

120 IT Interception Rules, R.10, https://indiankanoon.org/doc/30809273/.

renewable for a period not exceeding 180 days.[121] There is also a Review Committee, which reviews directions made by the competent authority.[122]

While this procedure is more detailed than Section 91 of the CrPC and is used for passing interception orders, police officials do not seem to rely on it to obtain data stored on company servers. This may be because a law enforcement agency cannot directly issue an interception direction under this provision: an authorised officer of the government will need to issue the direction first. In that sense, the direction for interception is given by an independent authority separate from the agency investigating a crime.

The IT Act does not specifically deal with access to evidence stored with foreign service providers.[123] Even if an interception direction were to be issued concerning a US service provider, such service provider would still be subject to ECPA restrictions on disclosing user data.

The IT Act does not specifically deal with access to evidence stored with foreign service providers. Even if an interception direction were to be issued concerning a US service provider, such service provider would still be subject to ECPA restrictions on disclosing user data.

121 IT Interception Rules, R.11, https://indiankanoon.org/doc/30809273/.

122 IT Interception Rules, R.22, https://indiankanoon.org/doc/30809273/. This Review Committee is the same committee set up under the Indian Telegraph Rules that also provide for interception of communication.

123 The Act does extend to any offence committed outside India by any person as long as the act constituting the offence involved a computer or computer network in India. IT Act, S. 75, https://indiankanoon.org/doc/576992/.

FORMAL REQUEST MECHANISMS BETWEEN INDIA AND THE US FOR CONTENT OF STORED ELECTRONIC COMMUNICATIONS

This chapter highlights another important component to address the frustration that Indian law enforcement face in accessing stored electronic communications held by US service providers: the existing formal request mechanisms that require multi-step processes in both India and the US and the inevitable time delays that result from such systems. We also further explain in detail the need for Indian law enforcement to understand the requirements of both the US legal system and the Indian legal system. Unless the request by Indian law enforcement contain sufficient details to comply with all of the legal requirements in the multi-step process in both India and the US the law enforcement entity that makes the request, through the formal request mechanism, may receive no evidence at all. This can be addressed in part by training and sensitisation for law enforcement at all levels to gain familiarity with legal requirements in both countries.[124]

This chapter describes the two existing formal request mechanisms between India and the US: the MLAT process and letters rogatory.

This chapter describes the two existing formal request mechanisms between India and the US - the mutual legal assistance treaty (MLAT) process and letters rogatory.[125] The discussion highlights the delays that typically result from each of these mechanisms. The chapter also examines concerns amongst certain agencies in India that MLAT requests cannot be made in the absence of an authorising statute expressly recognising MLATs.

A. The MLAT process, the most commonly used formal request mechanism, takes an estimated average of at least 10 months (global average) for law enforcement to receive electronic evidence

A MLAT is a formal agreement between countries to seek and exchange evidence located in their jurisdictions upon requests from another country that is party to the treaty.[126] Typically, the relevant evidence, whether physical, electronic, or testimonial, is related to criminal activity and is sought to aid law enforcement in the requesting state.[127]

---

124 This report describes the processes and requirements in both US and India with a view to facilitating successful requests for assistance. See Chapter II for procedures and requirements in US law and Chapter III for a discussion on Indian procedures. For a discussion on other avenues for cooperation, see Chapter V of the report.

125 In this paper, our focus has largely been on requests originating in India and how they are dealt with in the US.

126 MLATs can be multilateral or bilateral.

127 MLATs generally cannot be utilised to seek evidence in the investigatory stages of civil proceedings. For civil matters, requests for evidence can be made to foreign governments via "letters rogatory," which are issued and received by courts, not central authorities, and are available to civil litigants. See Section B of this chapter for details. For an explanation of how letters rogatory are handled in the US, see T. Markus Funk, "Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges," Federal Judiciary Center International Litigation Guide, Federal Judiciary Center (2014): 1-4, 17-22. https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf.

On October 17, 2001, approximately one month after the September 11 attack on the US, the India-US MLAT was signed with both states emphasising increasing bilateral cooperation on counter-terrorism.[128] The India-US MLAT allows the two countries to offer the "widest measure of mutual assistance" to each other in the investigation and prosecution of terrorism, narco-trafficking, economic offences and organised crime.[129] Political offences and crimes under military law are excluded from the scope of assistance envisaged, subject to a few exceptions including crimes against heads of states.[130]

The MLAT designates one central authority in each country to process incoming requests.[131] In the US, the designated central authority is the Office of International Affairs at the US Department of Justice (DOJ) or a person designated by the DOJ. In India, the central authority is the Ministry of Home Affairs (MHA) or a person designated by MHA.[132] Incoming requests are received by the central authority within the executive branch and are executed with the cooperation and approval of the competent federal court.

An Indian investigating agency seeking evidence in the US would submit a request to the MHA.[133] The MHA would then examine the request for compliance with the treaty and laws of the requested state and would send the request to the DOJ. On receiving an MLA request, the DOJ will ensure that the incoming request is consistent with US constitutional protections, including the Fourth Amendment probable cause requirement (described in the previous section). The DOJ will also examine whether the request is consistent with First Amendment speech protections. The DOJ reviews incoming MLA requests to screen out evidence that will be used to prosecute speech crimes, such as criminal libel, political dissent, or blasphemy.[134] When a service provider provides evidence to send to the requesting country, a First Amendment review is conducted once again to screen out production of specific documents or other evidence that would violate First Amendment speech protections.[135]

As the multi-step process in two different countries suggests, the MLAT process is lengthy. A 2013 US official report found that the average time from start to finish for this process is an estimated average of at least 10 months.[136]

---

128 "India, US sign treaty on legal assistance," The Hindu, 17 October 2011, http://www.thehindu.com/thehindu/2001/10/18/stories/01180005.htm. During this period after the US terrorist attacks on 11 September 2001, both the governments had also formalised their intelligence sharing mechanisms and resolved to cooperate on matters of cyber-terrorism and information security. Afroz Ahmad and Najish, "Before and After 9/11: Indo-US Counterterrorism Cooperation," Journal of International and Global Studies 9(2), no. 127, 130-131 (2017), http://www.lindenwood.edu/files/resources/127-138-before-and-after-9-11.pdf.

129 "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," 17 October 2001 ("India-US MLAT"), Preamble and Article I. Full text of the treaty can be found at this link: http://cbi.nic.in/interpol/mlat/UnitedStatesofAmerica.pdf.

130 Article 3(1), India-US MLAT.

131 Article 2, India-US MLAT.

132 India-US MLAT; The DOJ is the department of the US federal government that is responsible for enforcing federal laws, investigating crimes, and managing the federal criminal justice system, including federal prisons.

133 "Mutual Legal Assistance Requests," https://www.mea.gov.in/mlatcriminal.htm.

134 Peter Swire and Justin Hemmings, "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program," NYU Annual Survey of American Law 71, no. 687, 735-736 (2017), https://annualsurveyofamericanlaw.org/wp-content/uploads/2017/04/71-4_swirehemmings.pdf.

135 Peter Swire and Justin Hemmings, "Mutual Legal Assistance in an era of Globalized Communications: The Analogy to the Visa Waiver Program," NYU Annual Survey of American Law 71, no. 687, 736 (2017), https://annualsurveyofamericanlaw.org/wp-content/uploads/2017/04/71-4_swirehemmings.pdf. In addition, the text of the India-US MLAT as such does not mandate "dual criminality," – a requirement that the crime being investigated in the requesting country also constitutes a crime in the requested state. T. Markus Funk, "Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges," Federal Judiciary Center International Litigation Guide, Federal Judiciary Center, 2014, 1-4, 17-22. https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf. In practice, however, dual criminality is generally important to whether an MLAT request made to DOJ will succeed. The full text of the section can be found here: https://www.law.cornell.edu/uscode/text/18/3512. 18 U.S.C. 3512 (stating federal judges may only issue search warrants to assist a foreign criminal investigation when the foreign crime being investigated would be considered punishable in the US by imprisonment for more than one year).

136 This statistic is an average for all requests from all countries, and no statistics related to specific countries were

The production of evidence in the MLAT process can be further delayed, or even result in no evidence being released to law enforcement, when the request is deficient.

The production of evidence in the MLAT process can be further delayed, or even result in no evidence being released to law enforcement, when the request is deficient. For law enforcement requests that do not contain sufficient information to comply with all of the legal requirements in the multi-step process in both India and the US, the process will be halted until the deficiency is resolved by the requesting law enforcement entity. If the deficiency is not corrected in a manner that will meet the requirements of the applicable country's legal protections, no evidence will be produced to the requestor.

B. The letters rogatory process, a lesser known formal request mechanism involving courts in each of the countries involved, is believed to take longer than the MLAT process

A letters rogatory process enables a court to issue letters of request to foreign courts or authorities for compelling production of a document.[137] The process involves an investigating officer making an application to an Indian criminal court for evidence that may be available in a different country. Before making an application, the investigating officer has to first obtain concurrence of the Ministry of Home Affairs (MHA).[138] To obtain the MHA's concurrence, the agency needs to share the particulars of the case, relevant sections of the law, the legal opinion of the Director of Prosecution (or senior most Law Officer), and an extract of provisions from the relevant MLAT/MOU. In addition, the application to the MHA must be supported with a declaration that the case under investigation is not of political, military, racial, or religious character. To the extent that a request for letters rogatory must be approved by the MHA, the process for making a request is similar to the MLAT process. Unlike MLATs though, India has a specifically designated bodies to assist investigating agencies with making requests for letters rogatory, the International Police Cooperation Cell (IPCC)[139] at the Central Bureau of Investigation (CBI).

On receiving an application from an investigating officer, the Indian court may issue a letter rogatory to a foreign court or authority that is competent to process the request. The letters rogatory are sent to the foreign court or authority through diplomatic channels, namely through Indian missions in the country.[140] The foreign court or authority may, after examining the request, compel the production of any document or thing that is relevant to the case and forward the evidence collected to the court issuing such letter.

It is worth noting that the recipients of requests through this process are under no treaty obligations to review or process letters rogatory, in contrast to the legal obligation to cooperate made in MLATs.

included. Richard a. Clarke, et. Al., liberty and security in a changing world: report and recommendations of the president' s review group on intelligence and communications technologies 227, 2013, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

137 In India, the legal basis for the issuance of a letters rogatory request is either within the ambit of an MLAT or a different Memorandum of Understanding between the two countries. In the absence of such agreements, the legal basis for the issuance of a letters rogatory request is reciprocity. Ministry of Home Affairs, "Comprehensive Guidelines for investigation abroad and issue of Letters Rogatory," 31 December 2007, https://mha.gov.in/sites/default/files/LR-170709.pdf. As per the MHA 2007 Guidelines, the investigating agency must send a self-contained proposal to the Internal Security Division (IS-II) at the Ministry of Home Affairs. At the state level, the request can be routed through the Home Department of the State.

138 Ministry of Home Affairs, "Comprehensive Guidelines for investigation abroad and issue of Letters Rogatory," 31 December 2007, para (c), https://mha.gov.in/sites/default/files/LR-170709.pdf.

139 The IPCC is the body within the CBI that handles investigations outside India and routes requests for informal enquiries with investigating agencies of other countries or Interpol.

140 Ministry of Home Affairs, "Comprehensive Guidelines for investigation abroad and issue of Letters Rogatory," 31 December 2007, https://mha.gov.in/sites/default/files/LR-170709.pdf.

Although we are aware of no public statistics that are maintained related to letters rogatory, our interviews lead us to believe that the process is even slower than MLATs.[141] As with MLATs, production of the electronic evidence sought by the Indian law enforcement in their request will be further delayed if the original request does not contain sufficient details to fulfil the legal requirements in both India and the US Unless the Indian law enforcement officer adequately supplements a deficient request, the evidence likely will not be received at all.

C. Current ambiguity in Indian law leads some to believe that the law only permits the usage of letters rogatory – the lengthier of the two processes

The authors learned through their interviews that some law enforcement agencies in India, including the CBI, choose not send requests through MLAT and instead continue to send court-issued letters rogatory requests that are expressly recognised under the CrPC.

Certain law enforcement entities in India perceive an ambiguity in the law that necessitates the use of the letters rogatory process, to the exclusion of the MLAT process. This perception exists for some despite the fact that India has entered into MLATs with 39 countries.[142] The authors learned through their interviews that some law enforcement agencies in India, including the CBI, choose not send requests through MLAT and instead continue to send court-issued letters rogatory requests that are expressly recognised under the CrPC.[143]

These law enforcement agencies believe that an MLAT is not enforceable in India unless a specific provision or statute in domestic law legally recognises the request.[144] According to this interpretation, Section166A of the CrPC,[145] known as the enabling provision for letters rogatory, acts to override other provisions in the Code. The specific language at the beginning of Section166A, "Notwithstanding anything contained in the Code," is the source of the concern, as it can be interpreted to mean that letters rogatory are the only legal way to access evidence abroad. Those who assert this view point out that the intention of the legislature in drafting the section was to empower criminal courts (and not investigating officers) to make official requests to obtain evidence located abroad.[146] In assessing this ambiguity in the law, it is worth noting

---

141 Despite the delay involved, the scope of evidence that can be collected through letters rogatory is believed by some scholars to be more expansive than MLATs because the procurement of evidence under MLATs is limited to what is permissible under the particular provisions of the treaty. See Amber Sinha et al., The Centre for Internet and Society, "Cross-Border Data Sharing: A Study in Processes, Content and Capacity," 27 September 2018, 21, https://cis-india.org/internet-governance/files/mlat-report.

142 Ministry of Home Affairs, "International Cooperation, Mutual Legal Assistance Treaties in Criminal Matters," https://mha.gov.in/division_of_mha/international-cooperation.

143 Section 166A of the CrPC enables a criminal court in India to issue a letter of request to a court in a different jurisdiction to require production of documents.

144 There are two views on whether international covenants or treaties entered into by the Government of India are binding in the same way as domestic law. One view is that a treaty does not automatically become part of domestic law and has to be implemented by legislation to take effect. For US readers, it is important to note that this view is different from the US approach where treaties are treated at par with federal law. The other view is that treaties can directly guide interpretation of rights and rules in India even in the absence of enabling law. See Vishakha v. State of Rajasthan (1997) 6 SCC 241, https://indiankanoon.org/doc/1031794/ (where the Supreme Court held that international conventions could be read into fundamental rights directly in the absence of domestic law occupying the field). Further, if there is a provision in domestic law that conflicts with a treaty provision, the domestic law provision is likely to prevail over the treaty although an attempt is first made to read the two harmoniously.

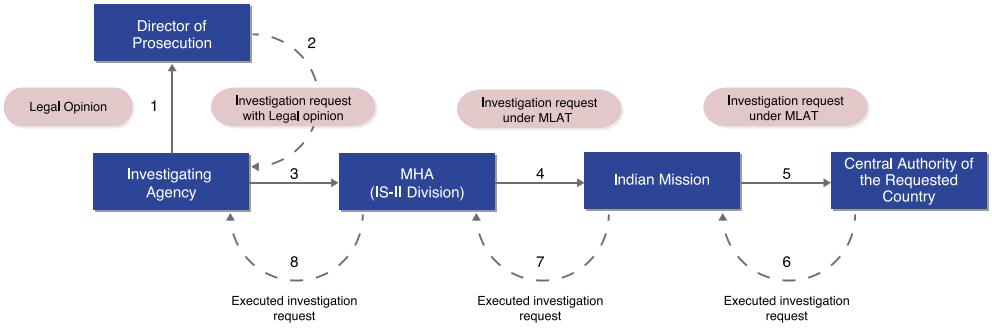
For a discussion on a proposed law to give effect to MLATs, see Gaurav Vivek Bhatnagar, "Easy Extradition: Letters Rogatory May Become Thing of the Past," The Quint, 1 December 2015, https://www.thequint.com/news/india/easy-extradition-letters-rogatory-may-become-thing-of-the-past.

145 "Notwithstanding anything contained in the Code, if, in the course of an investigation into an offence, an application is made by the investigating officer or any officer superior in rank to the investigating officer that evidence may be available in a country or place outside India..." S.166A of the CrPC, https://indiankanoon.org/doc/692989/.

146 In 2002, the High Court of Madras in the case of Jayalalitha v. State supported this view ruling that the letters rogatory

that some other agencies, such as the National Investigation Agency (NIA)—the central agency established to handle terror-related crimes—reportedly regularly send requests through the MLAT mechanism.[147]

To clarify this ambiguity regarding the legality of MLAT requests, the NIA requested the MHA to initiate a draft law on "Mutual Legal Assistance in Criminal Matters"—specifically concerning Malaysia, Singapore and Canada. The government was considering a domestic legislation recognising MLATs that would provide legal sanction to evidence obtained through MLATs and remove doubts about using the MLAT process.[148] The Bureau of Police Research and Development (BPR&D) in consultation with the NIA and CBI prepared the draft MLA Bill in 2015. The draft bill was based on the 2007 UN Model Treaty on MLA[149] and domestic laws in other jurisdictions and enabled parties to seek and provide legal assistance at any stage of a criminal matter, from investigation to appeal. The draft legislation, which is currently not available in the public domain, is said to have not progressed due to bureaucratic inertia and lack of support from the MHA.[150]



Indian side of the MLAT request

procedure under the statute cannot be supplemented by any other procedure. The court decided that there can be no justification in "adding or ignoring any word to make the provision more or less stringent than the legislature has made it." Jayalalitha v. State, 2002 Cri LJ 3026, https://indiankanoon.org/doc/151090791/.

147 The NIA also uses the letters rogatory process in cases where India does not have an MLAT with the concerned foreign state – for instance, the agency sent a letters rogatory to Pakistan in connection with the murder of two local leaders from the BJP Party. The NIA in the same case also issued a request under the India-South Africa MLAT. Saeed Khan, "NIA court sends Letter Rogatory to Pak govt for Bharuch double murder case", The Times of India, 30 March 2016, https://timesofindia.indiatimes.com/city/ahmedabad/NIA-court-sends-Letter-Rogatory-to-Pak-govt-for-Bharuch-double-murder-case/articleshow/51613794.cms. During the investigation of the 26/11 terror attacks in Mumbai, the NIA relied on the India-US MLAT to access evidence on the Headley-Rana case – the evidence finally formed a part of the charge sheet filed by the agency. On the other hand, the agency sent a letters rogatory to Pakistan in the same case to obtain evidence from the country. See NIA Press Release, http://www.satp.org/satporgtp/countries/india/document/papers/2012/National_Investigation_Agency_Release.pdf.

148 Express News Service, "Looking at legal protection for anti-terror ops: Rajnath Singh," The Indian Express, 13 August 2016, https://indianexpress.com/article/india/india-news-india/looking-at-legal-protection-for-anti-terror-ops-rajnath-singh-2971751/

149 Model Treaty on Mutual Assistance in Criminal Matters, http://www.unodc.org/pdf/model_treaty_mutual_assistance_criminal_matters.pdf.

150 See discussion in Chapter VII, infra, suggesting usefulness of clarifying the statutory basis to enable MLAT requests.

EXISTING MECHANISMS FOR COOPERATION AND INFORMATION-SHARING OUTSIDE OF MUTUAL LEGAL ASSISTANCE

In the previous chapter, we have described the formal request mechanisms for seeking access to stored communications and the steps involved in making a successful request for assistance. We now turn to the often overlooked existing cooperation and information gathering mechanisms between Indian and the US outside of the MLA process. These current channels can help address some of the frustrations currently faced by Indian law enforcement who seek to access stored electronic communications held by US service providers. The existing mechanisms have the potential to function as building blocks for addressing a variety of issues that arise in cross-border data transfers. The two categories of mechanisms include: a) methods currently available for cooperation and information sharing between India and US service providers; and b) methods currently available for bilateral and multilateral cooperation and information-sharing involving India and the US.

A. Methods currently available for cooperation and information-sharing between India and US service providers

This section of the report examines a legal avenue that Indian law enforcement can take to directly interact with US service providers – without the involvement of a formal request mechanism, such as MLATS or letters rogatory, or even coordination of the US government. Indian law enforcement can seek non-content data, including basic subscriber information and meta-data, directly from a US service provider. Here, we discuss mechanisms developed by service providers such as Apple, Google, and Facebook, which enable law enforcement agencies outside the US to make direct requests concerning such data.

1. Making requests under provider's Terms of Service, such as for non-content data, is an existing avenue of cooperation between Indian law enforcement and US service providers

A focus of concern for Indian law enforcement has been the restrictions on US service providers in disclosing content data to law enforcement agencies. As discussed above, service providers are not permitted to disclose the content of communications to US or non-US law enforcement except through a warrant or an appropriate request through a formal request mechanism like MLAT.[151] By contrast, US service providers may legally respond to other requests from non-US law enforcement, notably for non-content data such as subscriber information and metadata. Within the US there are legal rules that require US government agencies to use a subpoena or other specified legal tools for metadata such as the list of phone numbers or email addresses with whom a suspect has communicated. By contrast, while they cannot be compelled to do

US service providers may legally respond to other requests from non-US law enforcement, notably for non-content data such as subscriber information and metadata.

151 See Chapter IV for a detailed discussion.

so, service providers can voluntarily disclose customer records and subscriber information to "any person other than a US government entity."[152] This enables service providers to disclose certain non-content data to non-US government or law enforcement agencies.

To assist law enforcement in investigations, service providers, such as Apple, Google and Facebook, have developed mechanisms for receiving direct requests for non-content data. The mechanisms, set out in the terms of service and policies of the service providers, describe how requests are to be made and the kind of requests that will be considered. These voluntary mechanisms provide an avenue for Indian law enforcement to interact with US service providers for non-content data that can help with investigations.

The procedures for law enforcement to make requests are set out in the terms of service or policies of the service providers. For instance, Apple states that it considers requests by email from government agencies if they are sent from an official email address of the agency concerned.[153] Apple has made available a template[154] for law enforcement agencies to describe the context of the request, supporting information (such as device serial number, Apple ID or email address), and the information requested from Apple. Importantly, a request for information by law enforcement is considered legally valid if "it has a precise legal basis in the domestic law of the requesting country" and relates to "prevention, detection or investigation of offences."[155]

Google provides user data in response to a valid legal process from non-US government agencies on a voluntary basis if the request is consistent with "international norms, US law, Google's policies and the law of the requesting country."[156] Similarly, Facebook's policy also provides for responding to legal requests from non-US agencies on a good-faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognised standards.[157]

This is a useful channel, through which Indian law enforcement could directly seek basic subscriber information and transaction data from US service providers. On a similar footing, another avenue where law enforcement could directly reach out to service providers relates to the takedown of content. Service providers, in their terms of service, notify customers of content that the companies prohibit on their platform, such as graphic content or content that depicts or promotes violence, especially when such violence targets distinct groups of people. Any person (user or non-user of the service) can report to the service provider content that violates the terms.[158] This means Indian law enforcement can seek the takedown of content of publicly available posts under the terms of service of a US service provider.[159] Indian law enforcement can

---

152 **18 U.S.C 2702(c)(6),** https://www.law.cornell.edu/uscode/text/18/2702

153 **"Legal Process Guidelines: Government & Law Enforcement outside the United States," Apple, Chapter II,** https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf.

154 **Template for Government/ Law Enforcement Information Request, Apple,** https://www.apple.com/legal/privacy/gle-inforequest.pdf.

155 **Examples of requests Apple considers to be legally valid and receives internationally are: "Production Orders (Australia, Canada), Tribunal Orders (New Zealand), Requisition or Judicial Rogatory Letters (France), Solicitud Datos (Spain), Ordem Judicial (Brazil), Auskunftsersuchen (Germany), Obligation de dépôt (Switzerland), (Japan), Personal Data Request (UK), as well as equivalent court orders and/or requests from other countries." "Apple Legal Process Guidelines: Government & Law Enforcement outside the United States," Chapter II,** https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf.

156 **"Legal process for user data requests FAQs," Google Transparency Report Help Center,** https://support.google.com/transparencyreport/answer/7381738?hl=en.

157 **"Data Policy," Facebook, See response to "How do we respond to legal requests or prevent harm?"** https://www.facebook.com/about/privacy.

158 **The terms of service usually do not restrict the identity of the person who can report content (any user or non-user can report content). Facebook provides a special portal for non-users to report content.** https://www.facebook.com/help/www/181495968648557. **Twitter has a special process for law enforcement and government officials to request that content be withheld in their country. See section on "Content removal requests" in "Guidelines for law enforcement," Twitter Help Center:** https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support#16.5.

159 **For issuing takedown requests, Indian law enforcement would have to follow the procedures set out in the Indian IT Act and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules,**

request takedown even where the US Congress could not prohibit the speech. A provider's terms of service may restrict speech that is protected under the First Amendment to the US Constitution because the First Amendment applies only to "state action," to decisions about speech that are imposed by government in the US[160] For example, Facebook's Community Standards contain a blanket prohibition on hate speech, even though the US Supreme Court does not recognise the First Amendment as containing an exception for hate speech.[161]

The channels described here—for seeking subscriber information and metadata and for the takedown of content—are an existing avenue for Indian law enforcement to directly interact with US service providers. In addition, law enforcement access to subscriber information and metadata is often an important step toward meeting the stricter standards for access to content. This standard is currently "probable cause," pursuant to an MLAT request. Going forward, as discussed in Chapter VI, Indian law enforcement access to subscriber information and metadata may prove useful in meeting the somewhat easier standard under the Cloud Act of "articulable and credible facts."

B. Methods currently available for bilateral and multilateral cooperation and information-sharing involving India and the US

The following existing methods for bilateral and multilateral cooperation and information-sharing will be discussed in this section: 1) the US Legat Office; 2) efforts to combat counter cyber crime; 3) counterterrorism efforts; 4) efforts to combat money laundering; and 5) INTERPOL.

1. The US Legat Office located in India is an existing avenue for cooperation between India and the US

As we explore the multiple varieties of co-operation, one challenge for Indian law enforcement has been a lack of expertise about how to draft an MLAT request to the US or otherwise seek cooperation from the US legal system. In response, there is an expert source of knowledge through the US Legat process, and we describe that now to assist an Indian audience to be aware of this potential source of helpful information.

The Legat programme can best be understood as a tool to assist in dealing with the globalisation of criminal evidence and the worldwide spread of terrorism. The Legat office in India was opened in 2000 and is located in New Delhi.[162] This regional office serves as a point of contact for India as well as Bhutan, Maldives, and Sri Lanka.[163]

The history of the Legat programme may be helpful to understand the types of cooperation available. For more than 75 years, the US has stationed Federal Bureau of Investigation (FBI) Special Agents in countries around the world to strengthen relationships with the law enforcement agencies and intelligence services of multiple countries in an effort to exchange information that is of mutual interest, to battle crimes that have cross-border aspects, and to

---

2009. The law requires that blocking of websites or takedown orders be made by a designated officer not below the rank of a Joint Secretary.

160 See Dawn Nunziato, "First Amendment Values for the Internet," First Amendment Law Review 13, no. 282, 2014 (describing and critiquing this First Amendment doctrine), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2995760; see also Lata Nott, "Free Expression on Social Media," Freedom Forum Institute, https://www.freedomforuminstitute.org/first-amendment-center/primers/free-expression-on-social-media/.

161 "Community Standards," Facebook, Part III.12, https://www.facebook.com/communitystandards/objectionable_content; Eugene Volokh, "The Supreme Court unanimously reaffirms: There is no 'hate speech' exception to the First Amendment," The Washington Post, 19 June 2017, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/19/supreme-court-unanimously-reaffirms-there-is-no-hate-speech-exception-to-the-first-amendment/?utm_term=.c4dbe7532fbf.

162 The Legat Office in India can be contacted by calling the US Embassy at 011-91-1-98-2419-8000. Asia Overseas Offices, FBI Legal Attaché Offices, FBI International Operations, https://www.fbi.gov/contact-us/legal-attache-offices/asia; see Federal Bureau of Investigation Legal Attaché Program, US Department of Justice, Office of the Inspector General, Audit Division, Audit Report 04-18, March 2004, Redacted and Unclassified, p. 5, https://oig.justice.gov/reports/FBI/a0418/final.pdf.

163 Asia Overseas Offices, FBI Legal Attaché Offices, FBI International Operations, https://www.fbi.gov/contact-us/legal-attache-offices/asia.

combat terrorism that has implications in more than one nation.[164] These US personnel are assigned to Legal Attaché offices, commonly known as Legat offices, in the host countries.[165]

Today, the FBI's Office of International Affairs (OIA) in Washington, D.C., manages the Legat programme. OIA keeps in close contact with INTERPOL, foreign police, and national and international law enforcement associations.[166] Each Legat office is established through mutual agreement with the host country and is located either in the US embassy or consulate in the host nation.[167]

Legat offices serve as liaisons between foreign governments and FBI headquarters (as well as US FBI field offices) when the US needs assistance from foreign countries or their law enforcement agencies. In addition, the foreign law enforcement agencies can use the Legat office to transmit their requests to the FBI for assistance with an investigation. In these ways, the Legat offices build networks to prevent crime as well as to locate and extradite international criminals and terrorists.

One focus of the Legat office in India is training.

One focus of the Legat office in India is training. In May of 2016, the Indian Legat office held a training for Indian officials who work in counterterrorism to assist them in understanding the process to request evidence from the US pursuant to the US/India MLAT. The two-day event was co-sponsored by the Indian Ministry of Homeland Affairs, the Mumbai police, the US Department of Justice, and the FBI.[168]

In September of 2016, a second training was held by the Indian Legat office to discuss countering terrorist Internet usage. The event focused on methods of investigating terrorism cases using the internet and social media as well as dealing with online terrorism. This two-day training was co-sponsored by the Indian Ministry of Homeland Affairs, India's National Investigation Agency, the US Department of Justice, and the FBI.[169]

Another focus of the Legat office in India is counterterrorism. The Legat offices can facilitate the rapid deployment of FBI Special Agents who are invited by the host country to assist with major events, such as the investigation of terrorist attacks.[170] In 2016, the FBI Legat Office and the US Department of Justice provided the Indian Government assistance regarding the ongoing investigation of the Panhankot Airbase attack.[171]

---

164 The title for law enforcement officers at the FBI is "special agent." Special Agents, FBI Jobs, t https://www.fbijobs.gov/career-paths/special-agents.

165 Legal Attaché Offices, FBI International Operations, available at https://www2.fbi.gov/contact/legat/legat.htm; see "FBI Commemorates 75th Anniversary of Legal Attaché in Mexico City," News, FBI National Press Office, 3 December 2015, https://www.fbi.gov/news/pressrel/press-releases/fbi-commemorates-75th-anniversary-of-legal-attache-in-mexico-city.

166 INTERPOL is the acronym for the International Criminal Police Organization, headquartered in Lyon, France, that facilitates cooperation among international police authorities. INTERPOL, https://www.interpol.int/. See Section B.5 of this chapter for a discussion on INTERPOL.

167 Overseas Offices, International Operations, FBI, available at https://www.fbi.gov/contact-us/legal-attache-offices/#8; see generally Legal Attaché Offices: History, FBI, https://www2.fbi.gov/contact/legat/history.htm.

168 US Department of Justice Provides Mutual Legal Assistance Training to Counter Terrorism Investigators in Mumbai, US Embassy & Consulates in India, US Mission India, 19 May 2016, https://in.usembassy.gov/u-s-department-justice-provides-mutual-legal-assistance-training-counter-terrorism-investigators-mumbai/.

169 Department of Justice and Indian Investigators Hold Workshop to Discuss Countering Terrorist Internet Use, US Embassy & Consulates in India, US Mission India, 9 September 2016, https://in.usembassy.gov/department-justice-indian-investigators-hold-workshop-discuss-countering-terrorist-internet-use/.

170 Federal Bureau of Investigation Legal Attaché Program, US Department of Justice, Office of the Inspector General, Audit Division, Audit Report 04-18, March 2004, Redacted and Unclassified, p. 8, https://oig.justice.gov/reports/FBI/a0418/final.pdf.

171 "US Gave 'Substantial Assistance' in Pathankot Probe: Embassy," The Economic Times, 19 May 2016, https://economictimes.indiatimes.com/news/defence/us-gave-substantial-assistance-in-pathankot-probe-embassy/articleshow/52348560.cms.

A potential future focus of the Legat office in India is combating cyber crime. In 2011, the FBI began a programme to place cyber Assistant Legal Attachés, or cyber ALATs, into Legat offices. These individuals offer technical support in cyber investigations and information-sharing (to eliminate duplication of resources used in an investigation). The cyber experts are also expected to assist the host countries with jurisdictional issues, legal processes, and cyber laws, as well as to explain the particular cyber threats that are involved in an investigation. Upon request, these individuals can facilitate cyber training for foreign partners.

2. Efforts to combat cyber crime are existing avenues of cooperation between India and the US

Fighting cyber crime is pervasively cross-border. Evidence related to cyber crimes is typically found in multiple jurisdictions, and a rapid response is needed to preserve electronic evidence.

By the early 2000s, nations around the world recognised that cyber crime had become a vexing issue that affected virtually all nations. Despite the impacts experienced by individuals, businesses, and governments in countries such as India and the US prosecution of these crimes was difficult for at least two reasons: one was that there were no international standardised definitions of cyber crime and the second was that the legal processes to transfer electronic evidence across borders were either non-existent or inadequate. To address these concerns, more than 70 countries signed the Budapest Convention.[172] Although India has not signed this treaty, India has nonetheless adopted national legislation that is contemplated under the treaty – laws that outlaw certain classes of cyber crime. Specifically, India has criminal provisions that outlaw the disclosure of personal information without the data subject's consent, damage to computers or computer systems, sending offensive emails, e-commerce frauds, child pornography, and cyber terrorism.[173]

Since the early 2000s, cyber crime has continued to increase in frequency and severity. Worldwide news commonly features reports of hacking, phishing, ransomware, and malware. According to a 2017 report featured in Forbes, India has the highest percentage of users subjected to attacks by ransomware: 9.6 percent.[174]

To combat cyber crime, the Data Security Council of India (DSCI), and India's Ministry of Communications & Information Technology (MCIT) have trained more than 25,000 local law enforcement agents since 2012 in techniques for cyber forensics and cyber crimes investigation.[175] A recent example of bilateral cooperation between India and the US was a 2016 joint training held in New Delhi to discuss methods of investigating terrorism cases using the internet and

---

172 The treaty was designed to ensure that each signator enacted laws to criminalise certain classes of cybercrime – including illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offenses related to child pornography, and offenses related to copyright infringement. In addition, the treaty contained provisions intended to have these nations adopt procedural laws to address collection of electronic evidence and movement of data across borders. Convention on Cybercrime, Section 1: Substantive Criminal Law and Section 2: Procedural Law in Chapter II: Measures to be Taken at the National Level, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf; see Signatures to Budapest Convention, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

173 Information Technology Act 2000, https://indiankanoon.org/doc/1965344/; see An Overview of Cyber Laws v. Cyber Crimes: Indian Perspective, Lexology, https://www.lexology.com/library/detail.aspx?g=c0dd03b8-fab9-4daa-be5b-40b723537899.

174 Kevin Murnanem "Cyber Security: The World's Best and Worst Presented with A Well-Designed Infographic, Forbes , 4 May 2017, https://www.forbes.com/sites/kevinmurnane/2017/05/04/cyber-security-the-worlds-best-and-worst-presented-with-a-well-designed-infographic/

175 5th Cybersecurity Awareness Workshop for LEA, https://www.dsci.in/content/5th-cybercrime-awareness-workshop-lea; DSCI Data Protection Outlook 2012-13, Cybersecurity, Engagement with the National Security Advisor (NSA) – Initiation of Public Private Partnership in Cybersecurity, Key Recommendation #6, p. 18 https://www.dsci.in/sites/default/files/DSCI-Annual%20Report-Data-Protection-Outlook-2012-13.pdf; see Data Security Council of India, https://www.dsci.in/; see also National Cyber-Forensics & Training Alliance (NCFTA) https://www.ncfta.net/; see CyFin, https://www.ncfta.net/Home/Cyfin.

social media as well as dealing with online terrorism. This event was co-sponsored by the Indian Ministry of Home Affairs, India's National Investigation Agency, the US Department of Justice, and the FBI.[176]

3. Counterterrorism efforts and other intelligence and military sharing are existing avenues of information-sharing between India and the US

Terrorism is tragically a topic that affects many countries in ways that are inextricably intertwined. Of all areas where cooperation is beneficial, counterterrorism efforts likely are the most critical to have a rapid response that is coordinated across multiple jurisdictions.

India and the US have engaged in joint counterterrorism efforts since 2001 – the year of the deadly terrorist attacks on the US Twin Towers in New York City.

India and the US have engaged in joint counterterrorism efforts since 2001, the year of the deadly terrorist attacks on the US Twin Towers in New York City. The India-US counterterrorism regime has an emphasis on the roles of central authorities in expediting and coordinating counterterrorism efforts.

Significant information-sharing efforts between India and the US include:

- In 2001, the two countries entered into an agreement was to create the India-US Joint Working Group on Counterterrorism. The goal of the Working Group was to encourage intelligence sharing on terrorist financial operations as well as joint training in border management, surveillance, and terrorist incident response.
- The Counterterrorism Cooperation Initiative (CCI), signed in 2010, provided a bilateral framework for both countries' counterterrorism units to engage in capacity-building, information-sharing and joint training, with a special focus on port and border security.[177]
- In June 2016, India entered into a pact with the US to benefit from US Homeland Security Presidential Directive-6 (HSPD-6)[178] and engaged in subsequent dialogue related to sharing lists of terror fugitives.[179] By signing HSPD-6, India and the US pledged to share terrorist screening information.[180]
- In August 2016, India-US counterterrorism cooperation further benefited from the signing of the Logistics Exchange Memorandum of Agreement (LEMOA), a measure to enhance military-

176 "Department of Justice and Indian Investigators Hold Workshop to Discuss Countering Terrorist Internet Use," US Embassy & Consulates in India, US Mission India, 9 September 2016, https://in.usembassy.gov/department-justice-indian-investigators-hold-workshop-discuss-countering-terrorist-internet-use/.

177 The Hindu Group, "India, US sign counter-terrorism initiative," The Hindu, 23 July 2010, updated 8 November 2016, http://www.thehindu.com/news/national/India-U.S.-sign-counter-terrorism-initiative/article16207465.ece.

178 "Homeland Security Presidential Directive/HSPD–6—Directive on Integration and Use of Screening Information To Protect Against Terrorism," 16 September 2003, US Government Publishing Office, https://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf.

179 President George W. Bush issued HSPD-6 in 2003 to consolidate a system for collecting and sharing terrorist screening information to aid counterterrorism efforts of the US and foreign governments.

180 Specifically, HSPD-6 provides for the mutual accessibility of signees' terrorist screening databases, subject to domestic laws and regulations. India's designated point-of-contact for terrorist screening is the Multi Agency Centre (MAC), an intelligence "fusion center" within the Intelligence Bureau (IB). See Sandy Gordon, India's Rise as an Asian Power: Nation, Neighborhood, and Region 34, 41, 2014. The US point-of-contact is the Terrorist Screening Center (TSC), a division of the Federal Bureau of Investigation (FBI). See "Review of the Terrorist Screening Center," US Department of Justice, Office of the Inspector General, Audit Division, June 2005, https://oig.justice.gov/reports/FBI/a0527/final.pdf. Information shared between MAC and the TSC includes suspected terrorists' names, nationalities, dates of birth, fingerprints, photographs, and passport numbers. Indian Express Group, "India-US to sign 2 key pacts during Homeland Security Dialogue," The Financial Express, 30 May 2016, http://www.financialexpress.com/economy/india-us-to-sign-2-key-pacts-during-homeland-security-dialogue/269397/.

to-military cooperation. LEMOA allows India and the US to use each other's military bases and, more broadly, deepens logistical cooperation in areas like counterterrorism.[181]

- More recently, in September 2018, India and the US signed the Communications Compatibility and Security Agreement (COMCASA) that will give the Indian military access to function on high-end secured and encrypted communication equipment installed on American platforms.[182]

- Formal arrangements for information-sharing and capacity-building have figured into broader diplomatic initiatives to harmonise and strengthen India-US counterterrorism cooperation. For example, a joint India-US statement issued in June 2017 after a meeting between President Donald Trump and Prime Minister Narendra Modi highlighted information-sharing with the Terrorist Screening Center as a milestone in India-US counterterrorism cooperation.[183] Modi and Trump expressed hopes to see further cooperation on counterterrorism, including mutual consultation in creating lists of designated domestic and international terrorists.[184]

- In a January 2018 policy address, US Ambassador to India Kenneth Juster discussed enhanced counterterrorism cooperation, highlighting "designation lists" of terrorists targeted for financial sanctioning as well as the inaugural US-India Counterterrorism Designations Dialogue of December 2017.[185]

- Open-source publications provide evidence that suggests that India-US counterterrorism cooperation has contributed to recent successes in India's efforts to prevent terrorism within its borders. Particularly, India's cooperation with US intelligence agencies has reportedly disrupted operations of al-Qaeda in the Indian Subcontinent (AQIS) and the Islamic State of Iraq and the Levant (ISIL). The US has designated, sanctioned, or removed AQIS leaders.[186] For example, in July 2016, the US designated AQIS as a Foreign Terrorist Organization and its leader Asim Umar as a Specially Designated Global Terrorist, authorising the US government to block Umar's network of financial support.[187] In a similar way, the US government helped combat ISIL's India operations when it designated Mohammad Shafi Armar as a Specially Designated Global Terrorist in June 2017. Armar is considered the top ISIL recruiter in India and has helped expand the terrorist organisation's operations in the country.[188]

---

181 The Times Group, "India and the US sign LEMOA: What it is about," The Times of India, 30 August 2016, https://timesofindia.indiatimes.com/india-and-the-us-sign-lemoa-what-it-is-about/listshow/53922533.cms.

182 Manu Pubby "India, US ink Comcasa deal at 2+2 dialogue," The Economic Times, 7 September 2018, https://economictimes.indiatimes.com/news/defence/comcasa-india-to-get-access-to-real-time-encrypted-information-from-us/articleshow/65710975.cms.

183 "Fact Sheets: The United States and India – Prosperity Through Partnership," The White House, 26 June 2017, https://www.whitehouse.gov/briefings-statements/fact-sheet-united-states-india-prosperity-partnership/.

184 "The United States and India: Prosperity Through Partnership," The White House, 26 June 2017, https://www.whitehouse.gov/briefings-statements/united-states-india-prosperity-partnership/.

185 "Full Transcript: Ambassador Kenneth I. Juster's Inaugural Policy Address," US Embassy & Consulates in India, 12 January 2018, https://in.usembassy.gov/full-transcript-ambassador-kenneth-justers-inaugural-policy-address/.

186 Pamela G. Farber and Alexander Powell, "Al-Qaeda in the Indian Subcontinent: An Al-Qaeda Affiliate Case Study," CNA (2017), 16-7: https://www.cna.org/cna_files/pdf/DIM-2017-U-016120-2Rev.pdf. The authors also state US has had limited success in dismantling AQIS training networks in India.

187 The US based this designation on information provided through intelligence-sharing arrangements with Indian agencies. Shubhajit Roy, "US puts chief of al-Qaeda in Indian Subcontinent on terror list," The Indian Express, 1 July 2016, http://indianexpress.com/article/india/india-news-india/us-puts-chief-of-al-qaeda-in-subcontinent-on-terror-list-2886961/; On 23 September 2001, President George W. Bush signed Executive Order 13224, which authorised the US government to block assets and financial support of individuals blacklisted as Specially Designated Global Terrorists. The criteria for this designation were outlined in the Executive Order. See "Executive Order 13224," Office of the Coordinator for Counterterrorism, US Department of State, 23 September 2001, https://www.state.gov/j/ct/rls/other/des/122570.htm.

188 The Hindu Group, "US names IS' top India recruiter a global terrorist," The Hindu, 16 June 2017, http://www.thehindu.com/news/international/is-india-recruiter-named-in-us-terror-list/article19077720.ece.

4. Efforts to combat money laundering and other financial schemes used to fund terrorist or criminal networks are existing avenues of information-sharing between India and the US

Money laundering is another subject that can only be handled with cross-border cooperation. Because evidence related to money laundering is often found in multiple locations, coordination between involved countries is key. The United Nations has called for countries to put in place harsh criminal sanctions for the financing of terrorist organisations.[189] In the most recent statement by the India-US Working Group on Counterterrorism, each side agreed to strengthening information-sharing practices to counter the financing of global terrorist networks.[190] As part of the US-India Economic and Financial Partnership (EFP), the two countries have agreed to work on tax disputes, anti-money laundering, and fighting the financing of terrorist networks.[191]

5. INTERPOL provides an example of international cooperation and information-sharing

Multilateral mechanisms exist for information exchange amongst countries, particularly among law enforcement as they deal with cross-border issues that affect criminal investigations. One of the best known of these is INTERPOL, the International Criminal Police Organization. INTERPOL serves as a network for mutual assistance between police authorities of different countries. Given its role in cross-border information-sharing, the functioning of INTERPOL is an important piece in discussing existing mechanisms for law enforcement agencies to access data. In this section, we describe the INTERPOL network, the existing tools for cross-border information-sharing, and the information that can be exchanged through this network. We also discuss the procedures in India for obtaining information using the INTERPOL network, and identify potential ways in which this network could be leveraged further.

INTERPOL serves as a network for mutual assistance between police authorities of different countries. Given its role in cross-border information sharing, the functioning of INTERPOL is an important piece in discussing existing mechanisms for law enforcement agencies to access data.

INTERPOL is an international organisation set up to facilitate police cooperation between different countries. It has 192 member countries[192] and is seated in Lyon, France. Each member country has a body serving as the National Central Bureau (NCB), which liaises with other law enforcement agencies in the country, with INTERPOL's General Secretariat,[193] and with the NCBs in other countries.[194] INTERPOL seeks to facilitate law enforcement information exchange by providing secure communication channels

189 Security Council Urges Strengthening of Measures to Counter Threats Posed by Returning Foreign Terrorist Fighters, Adopting Resolution 2396, 21 December 2017 (call for countries to establish serious crimes for "financing of foreign terrorist fighters"), https://www.un.org/press/en/2017/sc13138.doc.htm.

190 Joint Statement on the 15th Meeting of the India-US Working Group on Anti-Terrorism, 27 March 2018, https://www.state.gov/r/pa/prs/ps/2018/03/279587.htm; see "Terror Discussed at India-US Meet," The Indian Express, 29 March 2018 (noting two sides discussed terror-funding), http://www.newindianexpress.com/nation/2018/mar/29/terror-discussed-at-india-us-meet-1794029.html.

191 See, e.g., Economic and Financial Partnership (EFP), Fact Sheet: US-India Economic Cooperation and People-to-People Ties, 2016 (increasing EFP's collaboration related to anti-money laundering and combating terrorist financing),https://in.usembassy.gov/fact-sheet-u-s-india-economic-cooperation-people-people-ties-june-7-2016/; Joint Statement on Sixth Annual US-India Economic and Financial Partnership (2016) EFP, which began in 2010, has a focus on resolving tax disputes between India and the US and sharing cross-border tax information), https://www.treasury.gov/press-center/press-releases/Pages/jl0424.aspx; see also "India, US Tighten Cooperation Against Illicit Money Flows," Reuters, 12 February 2015, https://in.reuters.com/article/india-usa-moneylaundering-idINKBN0LG19320150212.

192 INTERPOL Member Countries, https://www.interpol.int/Member-countries/World.

193 INTERPOL Constitution, Article 25, https://www.interpol.int/About-INTERPOL/Legal-materials/The-Constitution. ("The permanent departments of the Organization constitute the General Secretariat.")

194 INTERPOL Constitution, Article 32, https://www.interpol.int/About-INTERPOL/Legal-materials/The-Constitution.

connecting NCBs in all member countries.[195] In India, the Central Bureau of Investigation (CBI), through its International Police Cooperation Cell (IPCC), has been designated as the NCB to act as a liaison with NCBs of other countries and Interpol headquarters.

NCBs are allowed to directly access INTERPOL systems and this access is enabled through a global communications system known as I-24/7.[196] NCBs can access this system after being authenticated through INTERPOL's authentication mechanism—this secure authentication system ensures that only authorised users can access the databases and communicate with other NCBs.

The IPCC in India is allowed such access; any other investigating agency or state police seeking leads or information from a different country can route requests through the IPCC. Direct access to the system includes directly consulting the INTERPOL databases; recording, updating, or deleting data in the databases; using INTERPOL's "notices" and "diffusions" to make requests for cooperation and alerts; and direct transmission of messages to NCBs in other member countries.[197] Each of these is discussed briefly to understand the types of information-sharing that can take place.

INTERPOL Databases: INTERPOL manages a range of databases including records on known international criminals, missing persons, fingerprints, DNA, stolen motor vehicles, firearms, and stolen and lost travel documents.[198] NCBs and other authorised users are allowed to search and cross-check data in these databases and also record or update data. Another tool available to member countries is a set of colour-coded notices that are international requests for cooperation or alerts sent by law enforcement in a member country. These requests for cooperation or alerts are submitted by the NCB in any country to INTERPOL's General Secretariat. The Secretariat examines these requests and if found compliant with relevant INTERPOL rules, publishes them and notifies all other NCBs.[199] Any NCB that has information relating to the person or purpose specified in the notice is expected to forward the data to the requesting NCB.

INTERPOL Notices: INTERPOL has a system of notices, each serving a different purpose. For instance, "red notices" are issued to seek the location and arrest of wanted persons for the purpose of extradition or other action.[200] "Yellow notices" are meant to help locate missing persons.[201] "Blue notices" request the collection of additional information about a person's identity, location or activities in relation to a crime.[202] Each of these has its own set of criteria for publication, for instance, red notices can only be published if the offence concerned is a "serious ordinary-law crime" but not for offences relating to behavioural or cultural norms or those relating to family or private matters.[203] Blue notices, that seek to obtain information about a person of interest in a criminal investigation, can be published if the subject has been convicted or charged, or is a suspect, witness or victim, and sufficient data relating to the investigation is provided.[204]

INTERPOL Diffusion: A similar alert mechanism known as "diffusion" is also available to NCBs. Like notices, these are used to request the arrest or location of an individual or additional information in relation to a police investigation but are sent directly by an NCB to other NCBs. Through INTERPOL channels, NCBs are also able to communicate directly with other NCBs through "messages," which would not be recorded in the databases unless the requesting NCB

---

195 **Strategic Framework 2017-2020,** https://www.interpol.int/About-INTERPOL/Priorities/Strategic-Framework2.

196 **Data Exchange,** https://www.interpol.int/INTERPOL-expertise/Data-exchange.

197 **INTERPOL's Rules on the Processing of Data, Article 6,** https://www.interpol.int/About-INTERPOL/Legal-materials. ("Processing Rules")

198 **INTERPOL Fact sheet: Databases,** https://www.interpol.int/INTERPOL-expertise/Databases.

199 **INTERPOL Processing Rules, Articles 77-79.**

200 **INTERPOL Processing Rules, Article 82.**

201 **INTERPOL Processing Rules, Article 90.**

202 **INTERPOL Processing Rules, Article 88.**

203 **INTERPOL Processing Rules, Article 83.**

204 **INTERPOL Processing Rules, Article 88.**

consents to such recording.[205] The INTERPOL communications system thus provides a useful channel for law enforcement in different countries to share leads.[206]

INTERPOL Nodal Points: The nodal points for all information exchanges and cooperation through the INTERPOL system are the NCBs in each country. INTERPOL has been seeking to extend access to other national agencies and frontline law enforcement offices, such as border guards. Such other institutions can be authorised to access the network by the NCB in the country subject to certain requirements, such as the institution in question being legally authorised to fulfil the role of a public institution in enforcing criminal law and the nature of its activities should not violate the aims or neutrality of INTERPOL.[207]

INTERPOL I-24/7: In India, investigative agencies seeking information abroad submit a request to IPCC which can access INTERPOL systems through I-24/7. Such requests to the IPCC should include the First Information Report (FIR) number,[208] names of accused and the offence that is being investigated along with other details relevant to the request.[209] India has, over the years, sought assistance in certain criminal investigations through INTERPOL. A recent example is issuing of a red notice for the arrest of Nirav Modi, a diamond merchant charged for bank fraud and money laundering by the CBI and the Enforcement Directorate in India.[210] Given that most criminal investigations are carried out by state police agencies, INTERPOL liaison officers have reportedly been designated in states from state Criminal Investigation Departments[211] to act as facilitators. It appears that the CBI (through the IPCC) continues to be the only body authorised to access the INTERPOL information systems and unlike some other countries, does not appear to have extended direct access to state or other law enforcement authorities in India.

At present, the INTERPOL system is not ordinarily used for sending MLA requests or responses. Some international conventions do allow state parties to transmit requests for MLA and related communication through INTERPOL in urgent circumstances.[212] INTERPOL and some European States, through an e-MLA project, are considering the use of INTERPOL's communication system for MLA requests.[213]

INTERPOL provide a useful mechanism for information-sharing and cooperation between law enforcement agencies in different countries. Information-sharing and communication is carried out through the secure global communication system I-24/7 which ensures only authorised users can communicate through the network. The tools available through this channel, including access to databases, notices, and direct communication with other NCBs, facilitate mutual cooperation between police agencies and can assist law enforcement in cross-border investigations.

---

205 INTERPOL Processing Rules, Article 9.

206 Such information that is gathered through communication with other countries' NCBs would still have to be proven as evidence if sought to be introduced in court.

207 INTERPOL Processing Rules, Article 21.

208 First Information Reports is a written document prepared by the police about the occurrence of an offence which starts off the investigation.

209 Ministry of Home Affairs, "Comprehensive Guidelines for investigation abroad and issue of Letters Rogatory," 31 December 2007, https://mha.gov.in/sites/default/files/LR-170709.pdf.

210 Devesh K. Pandey, "Interpol issues Red Notice against Nirav Modi, brother, employee," The Hindu, 2 July 2018, https://www.thehindu.com/news/national/interpol-issues-red-notice-against-nirav-modi/article24309184.ece.

211 Specialised wings in the state police.

212 For eg., see the United Nations Convention against Transnational Organised Crime (A/55/3823, entered into force in 2003), Article 18(13),

213 The e-MLA project seeks to examine the legal feasibility of creating a dedicated virtual global network allowing secure electronic transmission in MLA matters. "International experts meet on electronic mutual legal assistance," INTERPOL, 21 September 2018, https://www.interpol.int/News-and-media/News/2018/N2018-097.

PROPOSAL FOR NEGOTIATING AN INDIA-US EXECUTIVE AGREEMENT UNDER THE CLOUD ACT

In the report to this point, we have explained an important problem for Indian law enforcement: the strict requirements under the US Electronic Communications Privacy Act (ECPA) to gain access to stored electronics communications held by US service providers. This Chapter proposes a solution to that problem – an Executive Agreement under the new US Cloud Act. To date, commentators have been sceptical about whether India would qualify for such an Executive Agreement.

We propose two innovative mechanisms, available under existing Indian law, that together would address some major concerns about whether India would qualify for a Cloud Act Executive Agreement. One mechanism would meet the Cloud Act requirements for individual law enforcement requests. In short, this mechanism would make a law enforcement request eligible under the Executive Agreement where a judge issues the order that meets the Cloud Act requirements, as is already available under Indian law. The second mechanism would meet the Cloud Act requirements for institutional safeguards applying to law enforcement requests. In short, this mechanism would identify "Qualified Entities" for Cloud Act requests: one or more designated agencies within India would set up institutional mechanisms to ensure compliance with the requirements of the Cloud Act. We believe that these two innovations would meet the two critical goals of India and the United States: fulfil legitimate law enforcement requests, while protecting privacy and civil liberties.[214]

We propose two innovative mechanisms, available under existing Indian law, that together would address some major concerns about whether India would qualify for a Cloud Act Executive Agreement. One mechanism would meet the Cloud Act requirements for *individual law enforcement requests.* ... The second mechanism would meet the Cloud Act requirements for *institutional safeguards applying to law enforcement requests.*

To put these proposals in context, the Chapter discusses the controversial topic of data localisation. A major rationale for current data localisation proposals is to assist law enforcement. Because Indian law enforcement encounters difficulties in accessing content held by US and other foreign service providers, data localisation would appear to address those concerns of Indian law enforcement. As just mentioned, however, this chapter proposes a workable path to an India-US Executive Agreement under the Cloud Act, which would enable India to address its priority law enforcement concerns. With an effective executive agreement in place, the major rationale for India data localisation would be addressed. An effective Cloud Act agreement, in other words, would meet law enforcement goals while greatly weakening the rationale for data localisation requirements.

214 Note that for companies processing data through entities in the EU, restrictions in other law such as the EU GDPR would continue to apply.

This chapter explains the US Cloud Act, as it would apply to a possible Executive Agreement with India, including a brief discussion of the political lay of the land in the US for reaching such an agreement. It next explains the two proposed mechanisms, which would address the biggest obstacles to India reaching such an agreement. The chapter concludes with a discussion of data localisation, including how a Cloud Act Executive Agreement would address the largest concern of those who have supported localisation.

A. Executive Agreements under the US Cloud Act

In March, 2018, the US Congress passed the Cloud Act.[215] The first part of the Cloud Act clarified the rules when the US Department of Justice (DOJ) seeks evidence located outside of the US. The second part authorised new Executive Agreements, to enable non-US governments to access evidence held by US service providers. Where an Executive Agreement is in effect, countries such as India would be able to go directly to service providers for stored content, without the need to use the MLAT process and get approval from a US judge that probable cause of a crime exists.

An important impetus for passage of the law was the Microsoft Ireland case then pending in the US Supreme Court.[216] In that case, Microsoft had objected to a DOJ request for the content of emails held in Ireland, and had succeeded at the appellate level based on a narrow statutory argument. The Cloud Act clarified the law, and rendered the pending case moot. The Cloud Act states that DOJ can require US service providers to provide evidence where there is "possession, custody, or control" within the US, regardless of where the data is physically stored. This "possession, custody, or control" standard had been the most prevalent understanding of prior law,[217] so the Cloud Act essentially reaffirmed the earlier understanding of DOJ powers.[218]

The part of the Cloud Act pertinent to this discussion, 18 U.S.C. § 2523, contains the new provision for Executive Agreements, consistent with an earlier proposal by the Cross-Border Requests for Data Project of the Georgia Tech Institute for Information Security & Privacy.[219] The Cloud Act states that the Executive Agreement must include designated safeguards both at the level of each individual request and at an institutional level. For the individual level, this would mean that each separate request is subject to certain requirements. At the institutional level, this would mean that the overall set of requests from a country, such as India, complies with safeguards over time.[220]

India and the US would negotiate specific terms for an Executive Agreement, which is much easier to approve than the revision to the India-US MLAT A treaty, to come into force in the US, requires approval by two-thirds of the US Senate. By contrast, an agreement under the Cloud Act would not require approval by the legislature. First, the US Attorney General, in consultation with the Secretary of State, would certify that the Cloud Act's requirements would be met under the

---

215 For a readable explanation of the Cloud Act, see Peter Swire and Jennifer Daskal, "What the Cloud Act Means for Privacy Pros," International Association of Privacy Professionals, 26 March 2018, https://iapp.org/news/a/what-the-cloud-act-means-for-privacy-pros.

216 United States v. Microsoft Corporation, https://www.oyez.org/cases/2017/17-2; see Sarah Jeong, "The Supreme Court Fight Over Microsoft's Foreign Servers Is Over," The Verge, 5 April 2018, https://www.theverge.com/2018/4/5/17203630/us-v-microsoft-scotus-doj-ireland-ruling.

217 See Sedona Conference, "Commentary on Rule 34 and Rule 45 "Possession, Custody or Control"," Sedona Conference Journal 17, no. 467, 2016, https://thesedonaconference.org/sites/default/files/publications/Commentary%20on%20Rule%2034%20and%20Rule%2045.17TSCJ467.pdf (for a discussion on how this standard has been applied by courts).

218 Eric Wenger "Does the Cloud Act Really Grant DOJ Sweeping New Powers?" Cross-Border Data Forum, 27 August 2018, https://www.crossborderdataforum.org/does-the-cloud-act-really-grant-doj-sweeping-new-powers/.

219 See Cross-Border Requests for Data Project, http://www.iisp.gatech.edu/cross-border-data-project; Peter Swire and Justin Hemmings, "Mutual Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program," NYU Annual Survey of American Law 71, no. 687, 2017, https://ssrn.com/abstract=2728478.

220 The general institutional requirements under the Cloud Act is that a government such as India must have "clear legal mandates and procedures governing those entities of the foreign government that are authorised to seek data under the executive agreement, including procedures through which those authorities collect, retain, use, and share data, and effective oversight of these activities. 18 U.S.C. 2523(b)(1)(B)(iv), http://www.crossborderdataforum.org/wp-content/uploads/2018/07/Cloud-Act-final-text.pdf.

Executive Agreement. Next, Congress would have 180 days to review the executive agreement. The agreement would then go into effect unless Congress enacted a new law to disapprove it.[221]

In general, each request under the Executive Agreement must afford "robust substantive and procedural protections for privacy and civil liberties." Each request must meet the following specific requirements:

Each request under the executive agreement must afford "robust substantive and procedural protections for privacy and civil liberties."

- *Requests be subject to independent review.* The request "shall be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order."
- *Particularised requests.* The request must target a specific person, account, address, personal device or other identifier. That is, the request cannot be for bulk collection of data or for a general warrant.
- *Serious crimes.* The request "shall be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism."[222]
- *Comply with domestic law.* The request shall comply with the domestic law of the country, in this case, India. In addition, "any obligation for a provider of an electronic communications service or a remote computing service to produce data shall derive solely from that law." That is, the Executive Agreement does not itself create any obligation for the company to produce evidence.
- *Requests based on "articulable and credible facts."* The request must show a clear factual basis for the individual request. Indian law enforcement would have to be able to articulate the reasons for targeting the evidence, and the reasons must be credible. This standard is less strict than the typical US standard of probable cause of a crime.
- *Prohibition on the use of data to infringe on freedom of speech, as well as requiring countries to meet human rights standards, such as a prohibition on torture.* This provision is designed to limit the use of direct requests to access data that would be protected by the US First Amendment's protection of free speech.[223] An example of speech-related crime would be prosecution for blasphemy.[224]

---

221 The Executive Agreement would be submitted to Congress, which would have 180 days to consider the agreement under special procedural rules. If Congress does nothing, then the Executive Agreement enters into effect for a period of five years. If both houses of Congress disapprove the agreement, and the President signs that disapproval, then the Executive Agreement would be blocked. If both houses of Congress disapprove the agreement, and the President vetoes the disapproval, then the agreement can still be blocked if two-thirds of both Houses of Congress vote to override the veto.

222 While "serious crimes" are not defined in the Cloud Act, certain offences specifically referred to in MLAT agreements and in the Budapest Convention on Cybercrime could serve as examples. See, for eg., Article 3 of the India-US MLAT, http://www.cbi.gov.in/interpol/mlat/UnitedStatesofAmerica.pdf; Articles 7-10 of the Budapest Convention on Cybercrime, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561. .

223 The First Amendment to the US Constitution reads, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances. US Constitution, Amendment I, http://constitutionus.com/#x1; see "What Does Free Speech Mean," US Courts, https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does; see also A.J. Willingham, "The First Amendment Does Not Guarantee the Rights You Think It Does," CNN Politics, 27 April 2017 (explaining that a social media platform can ban a user without it being a First Amendment issue), https://www.cnn.com/2017/04/27/politics/first-amendment-explainer-trnd/index.html.

224 In India, insulting religion or religious beliefs, with deliberate and malicious intent to outrage religious feelings, is an offence punishable with imprisonment up to three years. Section 295A of the Indian Penal Code, https://indiankanoon.org/doc/1803184/ .

As discussed further below, in connection with the institutional safeguards within Qualified Entities, each individual request also must follow requirements relating to "US persons" (US citizens and lawful permanent residents). The Executive Agreement must prohibit direct or indirect targeting of US person data. The non-US government is prohibited from sharing evidence gained under the Executive Agreement back to the US unless it relates to significant harm, or the threat of such harm, to the US or US persons. For incidental collection of US person data—data collected, for instance, when an Indian national e-mails a US person—there must be "minimisation" procedures in place. (Essentially, minimisation means that the identity of the US person must be redacted before it is disseminated.) These rules about US persons reflect the idea that the US protections in ECPA should continue to protect US citizens and residents. By contrast, the US has less reason to insist on US standards when a foreign government is seeking the data of non-US persons, where the data is held by a US provider.

These requirements relating to US persons illustrate that the Executive Agreement, to qualify under the Cloud Act, must have institutional protections in place. Notably, those requesting the data must have procedures in place to minimise the data. Foreign governments that wish to enter into an Executive Agreement under the Cloud Act must also demonstrate broader institutional protections, including "respect for the rule of law and principles of non-discrimination."[225] In addition, DOJ is required to review a country's compliance with the Cloud Act requirements every five years, so there must be a mechanism to enable that periodic review. The foreign country should also demonstrate a commitment to promote and protect the global free flow of information and the "open, distributed, and interconnected nature of the Internet."[226] An Executive Agreement must also provide for reciprocal access. The foreign government should allow reciprocal rights of data access allowing service providers to respond directly to a request by a US government entity.[227] The Cloud Act has clarified that service providers in the US are required to provide evidence within their "possession, custody, or control" regardless of where the data is physically stored.[228] Instances may arise where US law enforcement is seeking evidence stored outside the US that is not within the possession, custody or control of a US service provider.[229] Under an Executive Agreement, the requirement for reciprocal access would enable US law enforcement to seek such data from an Indian service provider directly, as specified in an Executive Agreement.

These requirements relating to US persons illustrate that the Executive Agreement, to qualify under the Cloud Act, must have institutional protections in place.

B. US political considerations for Cloud Act Executive Agreements

The political debates during the passage of the Cloud Act provide context for understanding what sorts of privacy safeguards will likely be necessary to gain US support for an Executive Agreement with India. Based on the US authors' experience,[230] it will be difficult to bring an Executive Agreement with India into effect unless there are good answers for privacy and civil liberties concerns.

---

225 18 U.S.C. 2523(b)(1)(B)(ii), http://www.crossborderdataforum.org/wp-content/uploads/2018/07/Cloud-Act-final-text.pdf.

226 18 U.S.C. 2523(b)(1)(B)(vi), http://www.crossborderdataforum.org/wp-content/uploads/2018/07/Cloud-Act-final-text.pdf. See Section F.2 of this chapter for a discussion on the relevance of this requirement in context of data localisation mandates implemented and being considered in India.

227 18 U.S.C. 2523(b)(4)(I), http://www.crossborderdataforum.org/wp-content/uploads/2018/07/Cloud-Act-final-text.pdf.

228 18 U.S.C. 2713, http://www.crossborderdataforum.org/wp-content/uploads/2018/07/Cloud-Act-final-text.pdf.

229 For instance, the US subsidiary of an Indian parent may not have possession, custody or control over records with the Indian parent.

230 Swire was Chief Counselor for Privacy in the US Office of Management and Budget under President Clinton, and Special Assistant to the President for Economic Policy under President Obama.

During consideration of the Cloud Act, many privacy and civil liberties groups announced strong opposition to the proposal, preferring to retain the existing MLAT system.[231] Critics of the executive Agreements highlighted issues discussed in this report, such as: judicial oversight for access requests;[232] orders targeted with specificity;[233] and requiring a clear standard, such as probable cause, for such orders.[234] Although these objections did not ultimately block passage of the bill, the concerns of privacy critics were taken seriously during Congressional consideration, leading to a number of changes in the final legislation.[235]

Other commentators, including Professor Jennifer Daskal and an author of this report (Swire), made the case that the Cloud Act would actually enhance privacy protections.[236] A principle reason is that non-US countries would have an incentive to modify their law enforcement procedures to meet the requirements in an Executive Agreement. In addition, as discussed further below, the creation of Cloud Act Executive Agreements would address some of the reasons countries consider implementing data localisation requirements. These two considerations—discussions about standards for law enforcement access and the debate about data localisation—are central to the approach we propose in this chapter.

Similar to the views of Daskal and Swire, leading technology providers also supported passage of the Cloud Act. These service providers have continued to describe the importance of retaining strong protections before turning over the content of their customers' communications. The companies do so in part to retain the trust of their customers, trust that customer data will not be provided to governments without a proper legal basis. The importance of strong protections has been emphasised, for instance, in the writing of Brad Smith, President of Microsoft, in "A call for principle-based international agreements to govern law enforcement access to data."[237] Smith announced six principles for international agreements on access to evidence. Amongst them are the same set of issues discussed here, on "prior independent judicial authorisation," "specific and complete legal process," and "required minimum showing" for each individual request.

Strict protections for the data about US persons have been another prominent theme in US political debates about these issues. The coalition letter of privacy and civil liberties groups said: "The bill would fail to protect the constitutional rights of citizens and others residing in the US"[238] As a matter of practical politics, members of Congress have strong reason to protect their own constituents against access by foreign governments. There is thus reason to believe that strong concerns would be raised unless any Executive Agreement contains effective protections against non-US government access to the communications of US persons, except under strict legal standards.

In conclusion, on the political context in the US, the text of the Cloud Act sets forth the extensive list of safeguards expected to apply in any India-US executive agreement. Additionally, there will

---

231 **Coalition Letter on the Cloud Act, 12 March 2018 (listing 24 organisations opposing the bill),** https://www.aclu.org/letter/coalition-letter-cloud-act.

232 **Sharon Bradford Franklin, "Left Out of the Party on Cloud Nine: A Response to Jennifer Daskal," Just Security, 13 February 2018,** https://www.justsecurity.org/52189/left-party-cloud-nine.

233 **For discussion by human rights groups of the US "abhorrence of general warrants," see Letter to US Justice Department Concluding White House Should Not Let UK Demand Private Data in US," 26 November 2018,** https://www.hrw.org/news/2018/11/26/letter-us-justice-department-concluding-white-house-should-not-let-uk-demand-private.

234 **Neema Singh Guliani and Naureen Shah, "The Cloud Act Doesn't Help Privacy and Human Rights: It Hurts Them," Lawfare, 16 March 2018,** https://www.lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them.

235 **Robyn Greene, "Somewhat Improved: The Cloud Act Still Poses a Threat to Privacy and Human Rights," Just Security, 23 March 2018,** https://www.justsecurity.org/54242/improved-cloud-act-poses-threat-privacy-human-rights/.

236 **Jennifer Daskal and Peter Swire, "Privacy and Civil Liberties Under the Cloud Act: A Response," Lawfare, 21 March 2018,** https://www.lawfareblog.com/privacy-and-civil-liberties-under-cloud-act-response.
Jennifer Daskal and Peter Swire, "Why the Cloud Act Is Good for Privacy and Human Rights," Lawfare, 14 March 2018, https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights.

237 **Brad Smith, "A call for principle-based international agreements to govern law enforcement access to data," Microsoft Blog, 11 September 2018,** https://blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data.

238 **Coalition Letter on Cloud Act, 12 March 2018,** https://www.aclu.org/letter/coalition-letter-cloud-act.

\Abe informed and vocal criticisms wherever a proposed Executive Agreement falls short of the statutory standards. Any such criticism may well be greater for the Congressional sessions of 2019 and 2020, where the Democratic Party now has a majority in the House of Representatives, and thus the ability to call hearings about any weaknesses in a proposed agreement. For these reasons, successful drafting of such an agreement should contemplate effective and workable ways to implement the Cloud Act's required safeguards.

Successful drafting of such an agreement should contemplate effective and workable ways to implement the Cloud Act's required safeguards.

C. Proposal for a Workable Path for an India-US Executive Agreement under the Cloud Act to streamline access to content of stored electronic communications for serious crimes

Executive Agreements under the US Cloud Act must meet requirements for individual requests and for institutional protections. This section is a proposal for a roadmap that could meet both of these requirements by: 1) utilising existing Indian procedures to meet the requirements for individual requests; and 2) designating Qualified Entities to meet the institutional requirements.

1. Existing Indian procedures may meet Cloud Act requirements for individual requests

Indian law does not generally require: judicial approval; detailed specificity in a court order; or a finding that a request has met a standard such as articulable and credible facts. These three types of safeguards, however, are expected elements under the Cloud Act for an individual request for content. The idea we propose is straightforward – existing law in India authorises those stricter procedures, even though the stricter procedures are not required.

We now turn to a proposal for how India could potentially leverage existing legal procedures to meet the Cloud Act requirements for each individual request. In brief, Indian law does not generally require: judicial approval; detailed specificity in a court order; or a finding that a request has met a standard such as articulable and credible facts. These three types of safeguards, however, are expected elements under the Cloud Act for an individual request for content. The idea we propose is straightforward – existing law in India authorises those stricter procedures, even though the stricter procedures are not required.[239] A Cloud Act request, therefore, could proceed only when the stricter, optional procedures are followed, likely without the need to pass new Indian legislation.

As discussed in Chapter III, Section 91 of the CrPC authorises judicial orders but does not require them. In general practice, a police officer in charge of a police station can compel the production of any "document or other thing" that is necessary or desirable for the purposes of an investigation or trial. Section 91 also authorises a second path: a court may issue summonses to require the production of documents. The Indian Supreme Court has noted that a police officer

239 Justin Hemmings, Sreenidhi Srinivasan and Peter Swire, "How Stricter Procedures in Existing Law May Provide a Useful Path for Cloud Act Executive Agreements," Cross-Border Data Forum, 16 November 2018, https://www.crossborderdataforum.org/how-stricter-procedures-in-existing-law-may-provide-a-useful-path-for-cloud-act-executive-agreements; Justin Hemmings and Sreenidhi Srinivasan, "Foundations of a Potential Executive Agreement Between India and the US, Digital Debates, CyFy Journal Vol. 5, 2018, 57-61, https://www.orfonline.org/wp-content/uploads/2018/10/Digital-Debates-Online-Launch.pdf.

can petition the court to compel the production of evidence "for the purpose of an investigation, inquiry, or trial."[240] In addition, Section 93 of the CrPC sets out three situations where a judge may issue a search warrant, including providing that a court can issue a search warrant if it has reason to believe that the target of the warrant would not produce the information sought pursuant to a Section 91 demand. We submit that using such a judicial procedure[241] could satisfy the Cloud Act requirement that the request "shall be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order."

The same reasoning would apply to the Cloud Act requirements of specificity (no general warrants). Section 93 permits general warrants where the information sought is not known to be in the possession of a specific person, or where the court believes the proceeding will be served by a general search or inspection. Importantly, in all instances of issuing a search warrant, the court can, "if it thinks fit," specify the particular place to which a warrant can extend.[242] While specificity in warrants is not mandatory under Indian law, courts do have the discretion to restrict searches to specific places. This provision allowing for a judge to specify the place to be searched is similar to the specificity requirement in the Cloud Act that a search warrant "identify a specific person, account, address, or personal device."[243]

The same analysis would appear to apply to the Cloud Act requirement that the request be based on "articulable and credible facts." Currently, requests under Sections 91 and 93 do not require such a factual showing. It appears, however, that Indian judges could include such a factual showing in their orders to produce evidence.

This analysis supports the following approach for an India-US Executive Agreement. India would be able to make a request directly to a US service provider where: (i) an Indian judge issues an order, with (ii) specificity and (iii) a factual showing of articulable and credible facts. Other Indian requests to a US service provider would not qualify for Cloud Act treatment.

This proposed approach illustrates a general approach that could potentially reconcile the Cloud Act requirements with Indian national law. [244] For India or other countries seeking Executive Agreements, a careful review of existing legal procedures and safeguards may reveal that these countries can meet more of the Cloud Act's requirements than is obvious on first glance. To date, discussions have largely assumed that countries must require something by legislation—such as judicial review—or else they could not qualify for an Executive Agreement. Under that view, qualifying for a Cloud Act Executive Agreement could be extremely difficult since a nation would have to change its law enforcement requirements for all cases, just to qualify for an Executive Agreement. For a country as large and diverse as India, changing police procedures nationwide would be a truly daunting task.

By contrast, the approach here would only require the stricter procedures for the cases where Indian law enforcement today must rely on the slow and burdensome MLAT process. For these cases, an Executive Agreement could authorise direct and faster access by India based on existing law. Without changing its statutes or introducing new statutes, India could thus make a request directly to the US service provider for those cases that meet the requirements of the Cloud Act Executive Agreement.

---

240 State of Orissa vs. Debendra N. Padhi (2005) 1 SCC 568, https://indiankanoon.org/doc/7496/.

241 See Section F of this Chapter for a brief discussion on concerns with this approach relating to judicial backlog in India.

242 Indian Criminal Procedure Code, S.93(2), https://indiankanoon.org/doc/983956/.

243 18 U.S.C. 2523(b)(4)(D)(ii), http://www.crossborderdataforum.org/wp-content/uploads/2018/07/Cloud-Act-final-text.pdf.

244 We highlight here the multiple procedures that the Indian government can use to access criminal evidence. The phenomenon we describe exists in US law as well. For example, the Right to Financial Privacy Act authorizes government access to evidence under the non-judicial administrative subpenas (sic) of Section 3405, or judge-ordered search warrants or judicial subpenas under Sections 3406 and 3407. The Electronic Communications Privacy Act similarly offers a judicial and a non-judicial option under 18 USC 2701(b): (i) an administrative or grand jury subpoena can seek evidence, where there is prior notice from the government to the subscriber or customer; or (ii) a court order from a judge is also available, without the requirement for prior notice.

2. Defining Qualified Entities to meet Cloud Act requirements for requesting institutions

Along with meeting Cloud Act requirements for individual requests, an Executive Agreement would need to meet the law's institutional requirements. To meet these requirements, our central idea is that the Executive Agreement designate "Qualified Entities" – institutions within India that provide the institutional safeguards required for Executive Agreements.

Along with meeting Cloud Act requirements for individual requests, an Executive Agreement would need to meet the law's institutional requirements. To meet these requirements, our central idea is that the Executive Agreement designate "Qualified Entities," institutions within India that provide the institutional safeguards required for Executive Agreements. The discussion here first analyses the institutional requirements under the Cloud Act. It describes the advantages and workability of the Qualified Entity approach, and then provides preliminary ideas about what Qualified Entities India may wish to designate under an Executive Agreement.

a. Institutional requirements of a Cloud Act Executive Agreement

The general institutional requirements under the Cloud Act is that a government such as India must have "clear legal mandates and procedures governing those entities of the foreign government that are authorised to seek data under the Executive Agreement, including procedures through which those authorities collect, retain, use, and share data, and effective oversight of these activities."[245] This text of "those entities of the foreign government" explains the emphasis in our proposal on what should be considered Qualified Entities.

The law also contains more specific requirements related to institutional controls, including:

- *Minimisation for US person data.* The foreign government must adopt "appropriate procedures to minimise the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement."
- *Other minimisation requirements.* The foreign government should "segregate, seal, or delete, and not disseminate material" unless it is necessary for acting against serious crime, including terrorism, or to prevent death or serious bodily harm.[246]
- *Secure storage of data.* "The foreign government shall promptly review material collected pursuant to the agreement and store any unreviewed communications on a secure system accessible only to those persons trained in applicable procedures."
- *Accountability and transparency.* The foreign government must have "sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data by the foreign government."
- *Five-year compliance review.* The foreign government must agree "to periodic review of compliance by the foreign government with the terms of the agreement." The statute requires such a review at least once every five years, when the original agreement expires and is subject to renewal.

---

245 18 U.S.C. 2523(b)(1)(B)(iv) (emphasis supplied), http://www.crossborderdataforum.org/wp-content/uploads/2018/07/Cloud-Act-final-text.pdf.

246 More completely, "the foreign government shall, using procedures that, to the maximum extent possible, meet the definition of minimisation procedures in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801), segregate, seal, or delete, and not disseminate material found not to be information that is, or is necessary to understand or assess the importance of information that is, relevant to the prevention, detection, investigation, or prosecution of serious crime, including terrorism, or necessary to protect against a threat of death or serious bodily harm to any person." 18 U.S.C 2523(b)(4)(g), http://www.crossborderdataforum.org/wp-content/uploads/2018/07/Cloud-Act-final-text.pdf.

This list of institutional requirements explains why a Cloud Act Executive Agreement with India would need careful attention in designating and managing Qualified Entities. An Executive Agreement must go beyond the requirements for an individual request, such as judicial order, specificity, and judicial showing. An agreement must also meet the institutional requirements to comply with the Cloud Act.

b. Advantages of the Qualified Entity approach

A 2017 article by Swire and Deven Desai provided an earlier version of the analysis here.[247] That article discussed the possibility of a "single point of contact" (SPOC) for Indian requests for content to US service providers. Now that the Cloud Act has been enacted, we revise the emphasis on single point of contact to include the possibility of multiple Qualified Entities.

The 2017 article highlighted the advantages of designating such an office rather than seeking to qualify all requests from Indian law enforcement. First, India can take the initiative in creating and defining one or more offices that would qualify. Compared with changing criminal procedure for all law enforcement for over a billion people, India can more realistically create and staff one or a few offices in the government that meet the Executive Agreement requirements. Second, the Cloud Act contemplates institutional controls, transparency, compliance, and oversight for a Qualified Entity that makes direct requests to service providers. Careful selection of Qualified Entities is more affordable and manageable than applying institutional requirements to all Indian law enforcement requests. Third, it is easier to authenticate requests from a Qualified Entity than from a multitude of different state and federal courts. Fourth, during periodic review of a Qualified Entity, a change in whether a particular office qualifies would have a confined effect, rather than disrupting practices of the entire national legal system.

c. Initial suggestions for constituting a Qualified Entity within the Ministry of Home Affairs' new Cyber and Information Security (C&IS) Division

The key point in our proposal is to highlight the importance of selecting an appropriate Qualified Entity that would be designated in an India-US Executive Agreement.[248] Here, we offer some initial suggestions for possible ways to proceed.

The key point in our proposal is to highlight the importance of selecting Qualified Entities that would be designated in an India-US Executive Agreement.

The Executive Agreement can name India's existing central authority for MLATs, the Ministry of Home Affairs (MHA)[249], as a Qualified Entity. The MHA at the centre controls all central police forces and special units, including the Indian Police Service (IPS), the elite leadership policecadre that holds senior ranks

247 Peter Swire and Deven Desai, "A Qualified SPOC Approach for India and Mutual Legal Assistance," Lawfare, 2 March 2017, https://www.lawfareblog.com/qualified-spoc-approach-india-and-mutual-legal-assistance.

248 As discussed above, the text of the Cloud Act applies to "those entities of the foreign government that are authorised to seek data under the executive agreement." 18 U.S.C. 2523(b)(1)(B)(iv) (emphasis supplied), http://www.crossborderdataforum.org/wp-content/uploads/2018/07/Cloud-Act-final-text.pdf. The Cloud Act thus leaves open the possibility of multiple Qualified Entities, but the proposal here is to designate a single Qualified Entity for India.

249 However, for implementing MLAT requests to date, our interviews found some concern that MHA has not been heavily staffed previously. There is thus some question about whether MHA, a ministry that is known to be burdened with various responsibilities, would receive the resources and institutional commitment needed to meet the institutional requirements described in the previous section.

in state police forces.[250] The Ministry has also been traditionally tasked with developing police capacity through training schemes and supplementing operational capabilities through use of technology.

The newly formed Cyber and Information Security Division (C&IS) under the MHA, set up in November 2017, appears best placed to adopt the role of a Qualified Entity.[251] The C&IS division consisting of multiple wings including a Cyber Crime wing and a Monitoring Unit, have been established to broadly undertake capacity building initiatives (of MHA officials and attached offices), set policies on cyber security and lawful interception, and cooperate with the Ministry of Electronic and Information Technology and Department of Telecommunications on policy related issues, and disseminate best practices on cyber crime prevention. Additionally, in early 2018, new sub-divisions under the C&IS, the Indian Cyber Crime Coordination Centre (I4C) and the Cyber Police Force were created to address the rising incidents of crimes online in India.[252] The I4C, among other responsibilities, has been specifically tasked with acting as a nodal point to coordinate all activities pertaining to the implementation of MLATs related to cyber crimes with other countries and suggest amendments in cyber laws to both keep pace with technologies and maintain international cooperation.[253]

It is our proposal that a separate committee be formed either under the I4C subdivision or under the overall C&IS division to route user data requests to US service providers directly and to meet the institutional requirements under the Cloud Act Executive Agreement. Given that policing is a state subject under the Indian constitutional framework, there is often a gap in cooperation between state and central law enforcement agencies.[254] Therefore, the committee that will be newly created should be represented by officers from all state police agencies.

The committee can be headed by a Director of IG rank (Inspector General of Police) and a Deputy Director of DIGP rank (Deputy Inspector General of Police). Officers of the Inspector or Sub Inspector ranks from state law enforcement agencies can be permanently appointed to the committee on a rotational basis. Four or more officers of the Deputy Superintendent of Police (DSP) rank who are specifically trained, could either be designated as zonal heads (representing the four different regions) or as subject-matter leads in priority areas. For instance, the police officer from Kerala can be designated as the lead for cooperation and data-sharing on online radicalisation and counterterrorism cases and a DSP from Telangana can be designated as lead

---

250 The Police Act V (1861) in India provides the statutory recognition for police agencies and lays out their responsibilities and functions. The Home Minister is accountable for all police actions to the Parliament at the centre. At the state level, the department of home in the state government controls state police forces and the state cabinet minister for home is said to be accountable to the state assembly. The Indian judiciary also weighs in on the scope of police powers in the country. For more on oversight and accountability of Indian police See Mario J. Aguja and Hans Born (eds.), "The Role of Parliament in Police Governance", DCAF, 2017, https://www.dcaf.ch/sites/default/files/publications/documents/The_Role_of_Parliament_in_Police_Governanc e.pdf. Suparna Jain and Aparajita Gupta, "Building Smart Police In India: Background into the Needed Police Force Reforms," http://niti.gov.in/writereaddata/files/document_publication/Strengthening-Police-Force.pdf
MHA has, on previous occasions, advised state governments to refer cases with cross-border implications to the CBI -owing perhaps to the specialised nature of its operations and the nature of investigations it usually carries out. Ministry of Home Affairs, "Advisory on Cyber Crime Prevention and Control," 13 January 2018, http://naavi.org/uploads_wp/new/mha_advisory_jan_2018.pdf.

251 Bharti Jain, "MHA forms two new divisions to check radicalisation, cyber fraud", The Times of India, November 10, 2017, https://timesofindia.indiatimes.com/india/mha-forms-new-divisions-to-check-radicalisation-cyber-fraud/articleshow/61595400.cms Additionally, the MHA division is launching a programme to train 37,500 police and law officers over the next two years on all aspects of tackling cybercrime. Azaan Javaid,"MHA to states: Gear up to counter cyber crime and phone fraud," Hindustan Times, February 16, 2018, https://www.hindustantimes.com/india-news/mha-to-states-gear-up-to-counter-cyber-crime-and-phone-fraud/story-ZMbCNSP6OuamCR3OlgapAL.html

252 "Union Home Minister reviews progress of newly created Cyber & Information Security (CIS) Division," Press Information Bureau, Ministry of Home Affairs, http://pib.nic.in/newsite/PrintRelease.aspx?relid=175699

253 The I4C scheme has been proposed with an outlay of Rs. 415.86 Crore and is said to run for two years."Details about Indian Cybercrime Coordination Centre (I4c) Scheme," Ministry of Home Affairs, https://mha.gov.in/commoncontent/details-about-indian-cybercrime-coordination-centre-i4c-scheme, the amount of money laid out for them

254 Indrajit Kundu, "Now, Mamata Banerjee blocks CBI's entry in Bengal, says fully support Chandrababu Naidu", India Today, https://www.indiatoday.in/india/story/mamata-banerjee-blocks-cbi-entry-west-bengal-1390242-2018-11-16

for cooperation for cyber crimes We suggest three priority areas where special representatives can be appointed:

a. Counterterrorism. The importance of counterterrorism, as well as the increasingly global aspect of terrorist organisations, make efforts related to combating terrorism an important area to prioritise in cross-border data flows between India and the US.

b. Cyber Incidents. Due to the multinational aspects of cyber crimes as well as the complexity of investigating these crimes and the need for rapid access to data in these investigations, the Indian government could consider a special cyber representative who could be the point person for related investigations. This representative can be the point of contact for cyber investigations with regard to programmes conducted in conjunction with the US Department of Justice's Office of International Affairs and the Criminal Division's Computer Crime and Intellectual Property Section.[255]

c. Anti-Money Laundering. The importance of combating money laundering, as well as the increasingly global aspect of the organisations involved in these criminal activities, make efforts related to fighting money laundering an important area to prioritise in cross-border data flows between India and the US. This is a third area where a special representative can be appointed in the Qualified Entity in MHA.

The special representatives can act as nodal points and ensure cooperation between the Qualified Entity and the requesting state or central agency to ensure data requests adhere to the Cloud Act requirements. Further, the MHA and the Ministry of External Affairs (MEA) can appoint a member at the Joint Secretary level to coordinate not just outgoing but also incoming requests under the Executive Agreement.

Such a Qualified Entity can also ensure that the individual request requirements such as judicial order, specificity, and judicial findings are met during outgoing requests. Instead of routing requests through individual state law enforcement agencies[256] state police can directly approach US service providers for evidence through the officer posted at the Qualified Entity in MHA.

If well implemented, requests from the Qualified Entity would meet strong standards for privacy and civil liberties enforcement, provide companies with greater certainty about which requests are lawful, and provide streamlined access to communications content for priority Indian law enforcement investigations.

E. Relevance of the Cloud Act proposal for the data localisation debate

The chapter thus far has examined how an India-US Executive Agreement could potentially operate under the Cloud Act. We next explore the relevance of this Cloud Act proposal for the controversial topic of data localisation. Law enforcement needs have been at the centre of current proposals to require data to be stored in India. A Cloud Act Executive

A Cloud Act Executive Agreement would directly address law enforcement concerns, thus strengthening the overall case against mandatory data localisation.

255 Office of International Affairs, https://www.justice.gov/criminal-oia; DOJ Cybersecurity Unit, https://www.justice.gov/criminal-ccips/cybersecurity-unit; Criminal Division's Computer Crime and Intellectual Property Section Celebrates 20 Years, Department of Justice, 21 October 2016 ("In 1997, the section helped form the G8 24/7 High Tech Crime Network, which created formal points of contact in participating countries for urgent assistance with international investigations involving electronic evidence."), https://www.justice.gov/opa/pr/criminal-division-s-computer-crime-and-intellectual-property-section-celebrates-20-years. 24/7 High Tech Crime Network, Computer Crime and Intellectual Property Section, http://www.oas.org/juridico/english/cyb20_network_en.pdf.

256 Routing requests through individual state agencies would likely be viewed with scepticism in the US. State authorities may not have sufficient legal authorities in place to meet Cloud Act requirements, and it would be difficult for the US to meet the statute's requirement for assessing and monitoring a larger number of Qualified Entities if state agencies were also authorised to directly send requests.

Agreement would directly address law enforcement concerns, thus strengthening the overall case against mandatory data localisation.

As part of its proposal for an Indian data protection law, the Srikrishna Committee Report would require that a copy of all personal data covered under the act be kept on a server in India.[257] The Report states that its proposal would allow law enforcement agencies to access information within their jurisdiction instead of "awaiting responses to requests made to foreign entities which store data abroad."[258] The localisation of data, in this view, would boost law enforcement efforts to access information for crime detection and for gathering evidence for prosecution.[259] Some in India view data localisation also as a means of exerting "data sovereignty," as opposed to having to comply with foreign legal requirements like demonstrating "probable cause."[260] Easier access to evidence has led several law enforcement agencies to favour data localisation.[261] It should be noted, however, that that for crimes with cross-border elements such as trans-national terrorism, cyber crime, and money laundering involving individuals and accounts that are not Indian, the data in question may not be stored in India and localisation would still not address law enforcement concerns.[262]

For other policy objectives, such as business growth and protecting privacy, there are arguments both for and against data localisation. Some writers have suggested that data localisation will help home-grown businesses, and attract investment in local IT infrastructure.[263] On the other hand, many voices from the business community have raised serious concerns about data localisation. For instance, Telangana's IT minister stated that the data localisation requirement in the draft data protection law would hurt Telangana's start-up businesses and discourage foreign investments in the state.[264] Other stakeholders have argued that data localisation could present a

---

257 The Srikrishna committee was set up to draft a data protection law for India. See Report on "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 2017, http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf ("Srikrishna Committee Report"). This Committee has proposed a data localisation requirement in the draft data protection law that is being considered by the Indian Government currently. The proposal requires that a copy of all personal data covered under the act be kept on a server in India. Clause 40 of the draft Personal Data Protection Bill 2018. The proposed data protection bill also authorises the Central Government to classify certain categories of "critical personal data" that can be processed only in a server or data centre located in India. This form of 'lockbox' localisation seeks to minimise the vulnerability of relying on undersea fibre optic cables and to prevent foreign surveillance of certain critical data. Srikrishna Committee Report Report, p.90, 93.

258 Srikrishna Committee Report, p.88.

259 Srikrishna Committee Report, p.88. Separate from these proposals, the banking regulator in India, the Reserve Bank of India (RBI), has mandated that payments data be stored exclusively in India. This covers all data relating to payment systems including "the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction." The RBI's stated goal for the measure is to ensure better monitoring and unfettered supervisory access to payments data. RBI Circular on "Storage of Payment System Data," 6 April 2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0.

260 According to news accounts, a panel headed by the co-founder of Indian tech giant Infosys, Kris Gopalakrishnan, which is responsible for drafting the Indian government's cloud computing policy has recommended that "Indian legal and policy frameworks must focus on ensuring that data generated from India can be utilised for the benefit of Indian citizens, governments and private players." As explanation, the draft report emphasised the importance of India securing "data sovereignty, especially in the context of cross-border data flows." Aditya Kalra, "Exclusive: Indian Panel Wants Localization of Cloud Storage Data in Possible Blow to Big Tech Firms," Reuters, 4 August 2018, https://in.reuters.com/article/us-india-data-localisation-exclusive/exclusive-india-panel-wants-localization-of-cloud-storage-data-in-possible-blow-to-big-tech-firms-idINKBN1KP08J.

261 Dalip Singh, "Law Enforcement Agencies Favour Data Localisation," The Economic Times, 8 October 2018, https://economictimes.indiatimes.com/news/economy/policy/law-enforcement-agencies-favour-data-localisation/articleshow/66113360.cms.

262 Bedavyasa Mohanty and Madhulika Srikumar, "Data localisation is no solution," ORF, 3 August 2018, https://www.orfonline.org/research/42990-data-localisation-is-no-solution/.

263 Shelly Singh and Dinesh Narayanan, "India's data localisation push can give rise to new business opportunity," The Economic Times, 25 October 2018, https://economictimes.indiatimes.com/tech/hardware/indias-data-localisation-push-can-give-rise-to-new-business-opportunity/articleshow/66356125.cms.

264 Surabhi Agarwal and CR Sukumar, "Telangana red-flags Data Protection Bill citing impact on startups, investments," The Economic Times, 13 September 2018, https://economictimes.indiatimes.com/news/economy/policy/telangana-red-flags-data-protection-bill-citing-impact-on-startups-investments/articleshow/65791116.cms; Bhumika Khatri, "Telangana

trade barrier for Indian start-ups looking to expand globally[265] and stifle technological innovation and growth that relies on the ability to transfer and replicate data in efficient ways.

For privacy protection, supporters of data localisation have suggested that it may help prevent surveillance of Indian citizens' data by foreign states.[266] On the other hand, data localisation would also create user and privacy concerns. Persons in India may be cut off from online services in other countries, where companies do not store data in India. Privacy advocates in India have also explained how localisation can lead to excessive access and surveillance by state authorities.[267]

In light of these recognised objections to data localisation, even proponents of localisation may seek to explore alternatives to reach the same goal, that of ensuring that law enforcement is able to access data necessary for investigations in a timely manner. An Executive Agreement under the Cloud Act, as explained in this chapter, would provide a new mechanism for Qualified Entities to directly request the content of communications from US service providers. In short, a perceived need for data localisation—readier access to evidence to investigate serious crimes—is answered by the Cloud Act proposal.

F. Potential concerns with an India-US Executive Agreement

In this chapter, we have described a proposal for an Executive Agreement between India and the US under the Cloud Act and highlighted ways in which it could be operationalised through existing legal structures in India and Qualified Entities. While this approach would boost law enforcement efforts to access data, there could be concerns both within India and the US surrounding such direct access. In this section, we highlight some of these potential concerns that may arise in developing an executive agreement between India and the US as well as responses to those concerns.

While this approach would boost law enforcement efforts to access data, there could be concerns both within India and the US surrounding such direct access. In this section, we highlight some of these potential concerns that may arise in developing an Executive Agreement between India and the US as well as responses to those concerns.

1. Concerns within India

We first discuss three potential concerns in India. First, under a Cloud Act Executive Agreement, US law enforcement would get reciprocal rights of access to data stored in India.[268] Preventing foreign surveillance is one of the reasons for localisation being considered in India.[269] A requirement for reciprocal access through a direct data-sharing agreement could raise concerns about US agencies obtaining data about Indian citizens. In response, it seems likely that an Executive Agreement would grant India considerably more access to US service providers than

Raises Concern On Draft Personal Data Protection Bill," Inc42, 13 September 2018, https://inc42.com/buzz/telangana-raises-concerns-on-draft-personal-data-protection-bill/.

265 Arindam Mukherjee, "Protection for Unruly Data," Outlook India, 2 August 2018, https://www.outlookindia.com/magazine/story/protection-for-unruly-data/300460; Aria Thaker, India's data localisation plans could hurt its own startups the most, Quartz India, 16 October 2018, https://qz.com/india/1422014/rbis-data-localisation-could-hurt-indias-own-startups/.

266 Dalip Singh, "Law enforcement agencies favour data localisation," The Economic Times, 8 October 2018, https://economictimes.indiatimes.com/news/economy/policy/law-enforcement-agencies-favour-data-localisation/articleshow/66113360.cms.

267 See, eg., Pranesh Prakash, "Why Data Localisation Might Lead To Unchecked Surveillance," Bloomberg Quint, 15 October 2018, https://www.bloombergquint.com/opinion/why-data-localisation-might-lead-to-unchecked-surveillance#gs.mt9buxo.

268 18 U.S.C. 2523(b)(4)(I), http://www.crossborderdataforum.org/wp-content/uploads/2018/07/Cloud-Act-final-text.pdf.

269 Srikrishna Committee Report, 90, http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

the US would gain in India. US service providers such as Facebook and Google currently have a large number of India subscribers, and Qualified Entities would gain direct access to content when following the Executive Agreement procedures. By contrast, the US currently already gains access to evidence where there is "possession, custody, or control" of the evidence in the US. While the scope of reciprocity would be defined under the Executive Agreement, it would likely primarily exist for US investigations where there is a subsidiary of an Indian company in the US, but the Indian parent holds the information. Even in that instance, the US government could likely request information from the parent, but could not compel it.[270]

In the future, however, this need of US law enforcement could likely intensify. With the Reserve Bank of India (RBI) imposing mandatory localisation on all payment system providers in the country and a reported 80% of the companies complying with these norms[271], significant user data will be stored in the country that may be valuable to US officials during investigations. The nature of the information stored will likely include that from international card networks, payment wallets and their Indian counterparts, Moreover, India has also unwittingly become a point of origin for global cyber attacks – with a reported fifth of all North Korean cyber intrusions now physically originating from India.[272] This too will make electronic evidence stored in India a rising priority for the United States and other affected states. Further, Indian startups in the tech sector are slowing expanding overseas, including the ridesharing company, Ola, which recently began operations in Australia, and budget hotels chain, OYO, who have now made inroads in China.[273] Therefore, to make a potential Executive Agreement under the Cloud Act future proof, US reciprocal rights to data stored with Indian intermediaries or service providers and the scope of their access should be an important topic during negotiations.

Second, the requirement to enable a periodic review may raise concerns about US interference in Indian internal affairs, a concern that has previously been highlighted in India-US discussions for entering into military and defence-related agreements.[274] In response, the Executive Agreement would provide for the limited scope of the periodic review – such review would apply only to Qualified Entities to the extent they request direct access to content from US providers. Such review may cover compliance with the Executive Agreement in general, but the Cloud Act's special focus for the review is on the treatment of evidence concerning US persons. This limited scope of review would appear an understandable trade-off for increased Indian access to important evidence for law enforcement investigations. It is especially understandable why the US would seek review concerning evidence pertaining to US persons.

Third, the proposal here anticipates that India would have to agree that direct requests to service providers be subject to "independent review" —a role for judges—as required by the Cloud Act. We have suggested an approach using existing legislative authorities in Indian law for judges to issue summons or warrant for requests. A concern facing such a proposal is the tremendous judicial backlog in India since courts in India already face capacity constraints.[275]

---

270 The Georgia Tech Cross-Border Access to Data Project is currently engaged in research on the scope and effect of the Cloud Act's reciprocity provision.

271 "RBI data localisation: 80% players comply with norms, say sources," The Economic Times, October 15, 2018, https://economictimes.indiatimes.com/industry/banking/finance/banking/rbi-data-localisation-80-players-comply-with-norms-say-sources/articleshow/66225263.cms

272 David E. Sanger, David D. Kirkpatrick and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More.", The New York Times, October 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

273 Ananya Bhattacharya ," India is just not enough for some Indian startups", Quartz India, June 25, 2018, https://qz.com/india/1311099/from-oyo-to-ola-indian-startups-are-going-international/

274 See Manjeet Sehgal, "India-US likely to sign agreements on information security, geospatial cooperation," India Today, 28 August 2010, https://www.indiatoday.in/india/story/india-us-likely-to-sign-agreements-on-information-security-geospatial-cooperation-1325585-2018-08-28.

275 Harish V. Nair, "3.3 crore backlog cases in courts, pendency figure at highest: CJI Dipak Misra," India Today, 28 June 2018, https://www.indiatoday.in/india/story/3-3-crore-backlog-cases-in-courts-pendency-figure-at-highest-cji-dipak-misra-1271752-2018-06-28.

Requiring judicial oversight for production of evidence would add to the burden on the court system and may be viewed with scepticism. In response to this understandable concern, we first note that the proposal would provide this role for judges only for direct requests for content to US service providers. Indian law enforcement could continue to request subscriber information and metadata from US service providers without judicial involvement. Law enforcement could also continue to use non-judicial procedures for requests to Indian and other non-US service providers. However, for the limited category of content requests to US service providers, Indian law enforcement would gain the advantage of making direct requests to the providers, without the need for a time-consuming Letter Rogatory or an MLAT request. In addition, Indian judges would face the Cloud Act standard of "articulable and credible basis" for the request, which appears to be at least somewhat easier to meet than the probable cause standard. An Indian law enforcement request to an Indian judge would thus appear to be considerably more timely and workable than the current, dysfunctional MLA process.

As an additional consideration within India, privacy advocates in India have been seeking stricter safeguards for the interception and collection of evidence by law enforcement and government agencies. An Executive Agreement under the Cloud Act can be seen as an opportunity to experiment, within a limited set of cases, with procedures that provide higher standards than current practice. As part of India's overall development of a new privacy regime, an executive Agreement can thus be a manageable initial step toward updated procedures for law enforcement access to evidence.

2. Concerns within the United States

We anticipate that the greatest objections to an India-US Executive Agreement would come from privacy and human rights advocates. As discussed earlier in this chapter, such advocates have sharply criticised the Cloud Act, both during its consideration in Congress and since. Currently, the US has been negotiating an Executive Agreement with the United Kingdom. In response, advocates have sent a letter criticising the U.K. for not having sufficient safeguards for law enforcement access.[276] One can thus anticipate similar, or even greater, concerns from these groups about a US-India Executive Agreement, especially if India does not provide the judicial review, requirements of specificity, and standard for request as discussed in the proposal here.

Concerns within the US would not be limited to privacy and human rights groups, however. As discussed above, Microsoft has announced quite strict principles for government access to users' data, and other major US service providers participate in efforts such as the Cross-Border Data Forum, which states as one of its organising principles: "protect and promote privacy and human rights as essential to new legal approaches."[277] Where advocacy groups and service providers share substantial concerns, then an Executive Agreement will be more difficult to negotiate and be subject to sharp criticism in Congress.

Any India-US Executive Agreement thus, to succeed, must be drafted to comply with the Cloud Act's legal requirements and in anticipation of careful scrutiny within the Congress. India's understandable incentive to seek the easiest possible access to content held by US providers should thus be tempered by a political realism about what the US will require by way of safeguards. For instance, it is unlikely that India will gain the ability to gain direct access to US providers to conduct wiretaps. That sort of real-time interception is treated especially strictly under US law and practice, with more than the usual probable cause requirements. Direct access to US providers for content will already be controversial within the US The condition for gaining such access will likely be to create procedures within India that provide the safeguards discussed here, notably judicial review, specificity, and evidentiary standard.

---

276 Trevor Aaronson and Sam Biddle, "New Law Could Give U.K. Unconstitutional Access to Americans' Personal Data, Human Rights Groups Warn," The Intercept, 26 November 2018, https://theintercept.com/2018/11/26/cloud-act-data-privacy-us-tech-companies.

277 Cross-Border Data Forum, https://www.crossborderdataforum.org. The Georgia Tech authors are engaged in work with the Cross-Border Data Forum.

In addition, as discussed earlier, the Indian government is considering a data localisation requirement for businesses. The Reserve Bank of India (RBI), India's banking sector regulator, has already imposed a requirement to store payments data on local servers.[278] One requirement for a foreign government to enter into a Cloud Act Executive Agreement is that the government be committed to an open Internet and to the free flow of information.[279] Localisation, according to scholars, goes against the idea of a free and open Internet.[280] To the extent India has implemented and is considering other proposals for localisation, it may fall short of the requirement of commitment to an open Internet and could be closing off the option of exploring an Executive Agreement with the US under the Cloud Act.

G. Conclusion

Observers to date have generally concluded that India would not qualify for an executive agreement with the US under the Cloud Act. This chapter, by contrast, has proposed concrete mechanisms for potentially overcoming some of the apparent obstacles. For judicial review and related safeguards, existing procedures exist under Indian law to enable the role for judges that the Cloud Act contemplates. For the concern that all of India would not be subject to strict new procedures, the discussion here has shown how designation of Qualified Entities could make the Cloud Act requirements manageable and effective.

Observers to date have generally concluded that India would not qualify for an Executive Agreement with the US under the Cloud Act. This chapter, by contrast, has proposed concrete mechanisms for potentially overcoming some of the apparent obstacles.

Once negotiated, an Executive Agreement would have notable advantages. Indian law enforcement would gain a streamlined new mechanism for directly requesting evidence from US service providers. Lack of such access has been a principle argument within India for data localisation. A Cloud Act Executive Agreement would thus meet a key law enforcement goal while reducing the rationale for data localisation. In addition, for privacy and human rights advocates, an Executive Agreement that complies with the Cloud Act would raise the level of safeguards for at least some investigations in India. This raising of protections would be consistent with India's current development of privacy rights, and it could make India a model for a more consistent regime in other nations as well for access to evidence.

278 The RBI has mandated that payments data be stored exclusively in India. This covers all data relating to payment systems including "the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction." RBI Circular on "Storage of Payment System Data," 6 April 2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0

279 18 U.S.C. 2523(b)(1)(B)(vi), http://www.crossborderdataforum.org/wp-content/uploads/2018/07/Cloud-Act-final-text.pdf.

280 See Anupam Chander and Uyên P. Lê, "Breaking the Web: Data Localization vs. The Global Internet," UC Davis School of Law, Working Paper 1, 2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858; Erica Fraser, "Data Localisation and the Balkanisation of the Internet," SCRIPTed 13(3), no. 359, 2016, https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/.

RECOMMENDATIONS

While preparing this report, we have examined numerous issues related to the delays experienced by Indian law enforcement in gaining access to stored electronic communications held by US service provides. We summarise here some recommendations.

The first two recommendations address steps to improve the operation of the current MLA system:

1. ***Resolve ambiguity regarding legality of MLATs:***

According to our research, there appears to be a current ambiguity in Indian law that leads some law enforcement agencies to believe that the law only permits the usage of letters rogatory, to the exclusion of MLATs. The authors take no position on the need for a law to provide for MLATs or its specific provisions, but do encourage Indian officials to resolve the uncertainty regarding the use of MLATs.

2. ***Resolve ambiguity regarding whether IT Act is the exclusive source of law for searches of the content of stored electronic communications:***

According to our research, there appears to be an ambiguity in the law regarding whether the IT Act governs the collection of the content of stored electronic communications, to the exclusion of the CrPC. The authors take no position as to the appropriate outcome of this legal ambiguity, but do encourage Indian officials to resolve the uncertainty.

The next three recommendations explore additional ways to foster India-US cooperation, for law enforcement as well as broader intelligence, military, or other purposes:

3. ***Provide additional trainings related to MLA requests and counterterrorism:***

The Indian Legat office has previously held a training for Indian officials who work in counterterrorism to assist them in understanding the process to request evidence from the US A second training was held by the Indian Legat office to discuss countering terrorist Internet usage. Pursuant to the India/US MLAT. Indian law enforcement could benefit by substantially increased training in what is needed to file a successful MLAT request.

4. ***Appoint a permanent Cyber Assistant Legal Attaché:***

Due to the globalisation of criminal evidence and the significant number of tech-related companies in India, DOJ could consider appointing a permanent cyber Assistant Legal Attaché assigned to India's New Delhi Legat office.

5. ***Explore using INTERPOL's authentication mechanism:***

Since the INTERPOL systems are an existing mechanism for authentication and secure communication, the use of this channel for MLA requests could be worth exploring. Another possible idea could be to use the existing secure INTERPOL channels for communicating with service providers directly for accessing non-content data, such as basic subscriber information, transactional data and metadata. Such requests are currently sent to service providers through portals operated by them. Using the existing INTERPOL channel that relies on authentication of law enforcement agencies could enable secure transmission of requests and responses, and would ensure that requests to companies are only forwarded from authorised agents and that requests follow the same template. However, since this would involve connecting service providers in some way to the INTERPOL systems, this suggestion is a significant change that would need further analysis.

Finally, these three recommendations would implement the proposals in Chapter VI for how an India-US Cloud Act Executive Agreement could operate:

6. Examine existing law to determine any gaps in existing authorities:

To meet the requirements concerning an individual law enforcement request, Chapter VI explained the technique of using stricter procedures under existing Indian law, such as judicial order, specificity, and judicial showing. Further research could identify any gaps in existing law, where it may be possible to augment current procedures with optional, stricter procedures to produce direct Cloud Act requests to service providers.

7. Constitute Qualified Entity within the Ministry of Home Affairs' new Cyber and Information Security (C&IS) Division:

Chapter VI explained that an Executive Agreement would need to meet the institutional requirements in the Cloud Act, such as controls on dissemination of evidence and oversight to ensure that the Executive Agreement is being followed. To carry out this approach with regard to institutional requirements, India may consider what organisations would best work as Qualified Entities. It is our proposal that the existing lead role of the Ministry of Home Affairs be retained and a Qualified Entity be constituted within the newly created Cyber and Information Security (C&IS) Division.

A permanent body housed within the MHA and consisting of representatives from the centre and each state should be the entity tasked with transmitting requests from all law enforcement agencies and ensuring centre-state cooperation in solving cross-border cases.

8. Examine the consequences of a successful Executive Agreement on the data localisation debate:

Proposals for mandatory data localisation have relied heavily on the law enforcement need to gain access to stored electronic communications held outside of India. The proposal for a Cloud Act Executive Agreement provides a mechanism to provide law enforcement access to such evidence, especially for priority and international investigations. Data localisation debates can be updated based on the path to a successful Cloud Act agreement described in this report.

CONCLUSION

In this Report, we have examined a problem that plagues Indian law enforcement, the problems of accessing the content of stored electronic communications held by US service providers. With data localisation being considered in India at the writing of this document, it is critical to address the problem of law enforcement access to evidence held outside the country.

We have examined the aspects of this problem that are shared by law enforcement officers around the world due to the globalisation of criminal evidence. In the discussion, we have examined the difficulty of complying with legal protections in two countries and looked at the inherent delays with MLATs and letters rogatory, both multi-step processes in two countries.

Part of the focus of the paper has been to examine the reasons that Indian law enforcement report both that they perceive the delays to be lengthier than other countries and that they perceive their requests to US service providers result in no release of information more often than requests by other countries. One apparent reason for these negative outcomes is sheer volume, with the number of Internet users in India being nearly double the entire population of the US. A second, more complex reason has to do with the US legal requirements for stored electronic communications. Fulfilling these requirements currently necessitates an in-depth understanding of US legal concepts such as "probable cause." It has been challenging for Indian law enforcement to understand the requirements of US law for MLAT requests. Where initial requests do not meet the unfamiliar US legal standards, an MLAT request must be supplemented, causing even more delay before receiving the requested evidence. If the modified request does not meet the US standard, the Indian law enforcement officer will not receive the requested evidence.

We believe one useful step to address the delay caused by the complexities of US law may be to provide additional training for Indian law enforcement about how to frame a successful MLAT request or request under the letters rogatory process. This type of training, in different languages, can take place within India, and may reduce frustration by showing achievable ways to get evidence that is lawfully available.

The US Cloud act offers an alternative to the requirement that requests by Indian law enforcement must comply with current US law. Although some commentators have lamented that an Executive Agreement between India and the US is not possible, our research leads us to be more hopeful. We have identified potential building blocks for the basics of such an agreement. One component would be to meet the requirements for each individual request. India may be able to leverage existing laws to create a process for law enforcement requests to the US that would comply with the requirements of the Cloud Act. The second component is to designate Qualified Entities as needed, which would have procedures to match the Cloud Act requirements. We have suggested that India might select priority offices to address cross-border crimes such as counterterrorism, cyber crime, and cross-border financial crimes such as money laundering.

We recognise that the road to an Executive Agreement between India and the US would be complex. Because the issues faced in India are experienced by many other countries around the world, we believe that the effort is worthwhile for India itself, and as a model for addressing many nations' problems posed by the globalisation of criminal evidence.