123

ORF SPECIAL REPORT

December 2020

ORF

CROSS-BORDER DATA FORUM

India's Access to Criminal Evidence in the U.S.: A Proposed Framework for an Executive Agreement

Peter Swire, DeBrae Kennedy-Mayo, Arjun Jayakumar

Getty Images / Andriy Onufriyenko

Attribution: Peter Swire, DeBrae Kennedy-Mayo and Arjun Jayakumar, "India's Access to Criminal Evidence in the U.S.: A Proposed Framework for an Executive Agreement," *ORF Special Report No. 123*, December 2020, Observer Research Foundation.

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

To know more about ORF scan this code

INTRODUCTION

This report is an introduction to a new research project of the Cross-Border Data Forum (CBDF) and the Observer Research Foundation (ORF) that aims to create a hub for discussions regarding Indian government access to electronic evidence held by US companies for criminal investigation purposes. The research seeks to identify current challenges to data-sharing between India and the US and outline the parameters of an executive agreement, as contemplated by the US CLOUD Act, that could be put in place to mitigate the challenges.[1]

The project builds on the 2019 Georgia Institute of Technology/ORF report, "India-U.S. Data Sharing for Law Enforcement: Blueprint for Reforms".[2] In this new project, legal experts from both the US and India will discuss the most crucial elements in promoting a legal system that would do the following:

- Fulfill legitimate requests from law enforcement agencies for data relevant to the investigation of serious crimes;
- Protect and promote privacy and human rights as essential to new legal approaches;
- Provide a workable regime for companies holding data that would be of interest to law enforcement agencies; and
- Safeguard the Internet by resisting calls to splinter it and localise data.[3]

Law enforcement agencies in India face serious obstacles to accessing electronic evidence held by ICT (Information and Communication Technologies) service providers based in the US. These issues were compounded in early 2020 when the Indian government—like many other governments across the globe—ordered a country-wide lockdown to combat the COVID-19 pandemic, interrupting essential services like public transportation and schooling, and commercial operations as well.[4]

As people in India turned to the Internet during the lockdown for their needs, it became more urgent to address cross-border data concerns to assist law enforcement investigations into criminal activity.[5] In this backdrop, an India-US executive agreement under the US CLOUD Act could provide a much-needed framework to ease the Indian government's access to data held in the US. Such a structure would not only facilitate the transfer of data

in connection with law enforcement investigations, but also safeguard user privacy and alleviate various concerns around lack of capacity within the government when it comes to accessing electronic evidence held overseas.

The provisions in the CLOUD Act will require careful consideration in any negotiations for the creation of an India-US executive agreement. The CBDF-ORF project will offer avenues for informed public discussions around the CLOUD Act and issues relevant to any eventual agreement. The project will welcome scholars and analysts from different fields to consider contributing their own publications on the subject of India's access to evidence held by US companies.

Part I of this report outlines the current challenges in India-US data sharing for law enforcement purposes, including difficulties that result specifically from the provisions of the US Electronic Communications Privacy Act (ECPA)[6] and the India-US Mutual Legal Assistance Treaty (MLAT).[7] Part II then explores a plausible remedy for the most severe problems in data-sharing, in the form of an India-US executive agreement under the CLOUD Act. Finally, Part III outlines the potential challenges in drafting such an executive agreement, and offers broad recommendations to address those hurdles.

I: INDIA-U.S. DATA SHARING: KEY CHALLENGES

The globalisation of criminal evidence has generated new challenges for law enforcement.[8] Consider a serious crime that takes place in Delhi, where both the perpetrator and the victim are located. Historically, any evidence about that crime would be expected to exist only within Indian territory, and subject only to domestic laws. Today, however, critical evidence—such as emails, social network communications, and even video—may be held by service providers based in the US, including social media companies and providers of cloud computing services, and therefore subject to US law.

To acquire this evidence, Indian law enforcement personnel face obstacles under procedures spelled out in both ECPA and MLAT. ECPA, for instance, bars US-based service providers from disclosing content of electronic communications to any law enforcement entity—whether local or foreign—unless certain requirements under US laws are fulfilled.[9] ECPA applies varying legal standards to different categories of electronic evidence: there are lower protections for those that reveal less information about the user (and therefore require less protection against potential abuses by law enforcement), and

higher protections are accorded to information that reveals more intimate details about the user (as there could be more intrusive violations by law enforcement agencies).[10] On the lower end of the spectrum, US providers are generally permitted to supply limited categories of *non-content* data (or metadata) to Indian law enforcement, such as basic subscriber information (BSI).[11] To acquire the *contents* of communications, ECPA requires that a request from the Indian law enforcement body meet the US legal standard of "probable cause"[12] that a crime has occurred and that evidence of such crime will be found during the search.[13] These US legal requirements apply to requests by Indian law enforcement even though the crime occurred outside the US, the victim and the suspect are not US citizens, and the electronic evidence is being requested by foreign law enforcement agencies.

Similarly, the India-U.S. MLAT process—often criticised for being slow and laborious—[14] poses additional obstacles to Indian law enforcement. To acquire evidence through the India-US MLAT process, Indian police must begin by filing an MLAT request with the Indian Ministry of Home Affairs (MHA). The MHA then relays an approved request to the Office of International Affairs under the US Department of Justice (DOJ). The DOJ then reviews the request and forwards it to a prosecuting attorney. After review, the prosecuting attorney brings the Indian MLAT request before a US federal judge. If the judge determines that the Indian request satisfies the relevant US legal requirements, the judge issues an order requiring the production of the documents by the US service provider. The company then produces the specified content, which subsequently must be reviewed by the US DOJ to ensure compliance with US laws. The US DOJ releases the permitted content to the MHA in India, and finally, the MHA provides the content to Indian police. Indian law enforcement agencies are tasked to supplement MLAT requests where the initial filing does not meet US legal standards, causing even more delay. If the modified request fails US standards, the Indian law enforcement officer will not receive the requested evidence.[15]

The process is lengthy and cumbersome, and impedes the swift and efficient performance of law enforcement investigators in India. On average, obtaining data from a US service provider using the MLAT process takes at least 10 months.[16] By some estimates, the process for Indian requests can take much longer to complete from service providers in the US, and can stretch to over three years on average.[17]

ORF's 2019 research found two key factors that influence these negative outcomes for Indian enforcement agencies. One reason has to do with the

complex US legal requirements for stored electronic communications. Fulfilling these requirements necessitates a clear grasp of US legal principles, such as that of "probable cause." Most investigations in India are routinely carried out by state police officers with some special crimes being handled by dedicated federal agencies. Even federal law enforcement officers in India may lack training to ensure compliance with foreign legal requirements. It has been challenging for Indian law enforcement agents to fulfill the unfamiliar requirements of US law for MLAT requests. A second reason for these current outcomes is the sheer scope and volume of internet activity: the number of Internet users in India is nearly double the entire population of the US.[18]

Further compounding these issues is speculation by some observers that the current number of MLAT requests from India to US service providers is artificially low.[19] Interviews conducted for this report indicate at least two potential reasons for the disproportionately low number of requests from India compared to its population. First, many law enforcement agencies in India may consider the MLAT process too slow and cumbersome to utilise at all. Second, the uncertainties under Indian law about the legality of the MLAT process affects its use by Indian law enforcement agencies.[20]

II: INDIA-U.S. DATA SHARING: DRAFTING AN EXECUTIVE AGREEMENT

The CLOUD Act creates a possible mechanism for addressing the obstacles faced by Indian law enforcement agencies under both the MLAT process and ECPA. If an executive agreement under the CLOUD Act is signed by India and the US, Indian law enforcement offices can make direct requests to US service providers for content of communications– eliminating the need to use the MLAT process. The basic concept of such an executive agreement is that non-US governments gain an exception to ECPA – thereby permitting their law enforcement agencies to request content directly – if a set of procedural, privacy and human rights protections applies to those requests.

An executive agreement would bring clear benefits to both India and the US. For Indian law enforcement investigations, this approach would allow direct access to content held by US service providers, where the terms of the executive agreement are satisfied. The US DOJ will also benefit from the executive agreement, as it would reduce its burden of processing MLAT requests coming from India.[21]

Notwithstanding the potential gains for both countries, however, there are issues that need to be addressed before such an executive agreement could be negotiated and implemented. To begin with, the CLOUD Act only permits direct access by a non-US government when institutional requirements and specific safeguards for individual requests are in place. The general institutional requirements under the CLOUD Act necessitate that a government such as India must have "clear legal mandates and procedures governing those entities of the foreign government that are authorized 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."[22] To meet these requirements, institutions within India would review requests and ensure that the overall program for making requests meets various institutional controls, such as "appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons."[23]

Furthermore, the CLOUD Act only permits direct access by a non-US government if a set of safeguards apply to each individual request.[24] For instance, there must be significant oversight by a judge, and not simply a request for evidence by a police officer, as is currently common in India.[25]

The implementation of this institutional infrastructure, and the accompanying safeguards, will therefore require appropriate amendments to existing Indian criminal and technology laws, as well as changes in current practice. There are two innovative mechanisms, available under existing Indian law, that together could address key concerns under the CLOUD Act for qualifying requests by Indian law enforcement agencies.

CBDF and ORF are undertaking this detailed study of a possible India-US executive agreement while recognising political concerns in both countries. In India, the concerns have focused primarily on the possible impacts of such an agreement. First, the requirement for reciprocal access for US law enforcement through a direct-access agreement may raise concerns about US agencies obtaining data on Indian citizens. Second, the requirement to enable a periodic review may raise concerns about US interference in Indian internal affairs. Third, the requirement that direct requests would be subject to judicial review could raise concerns related to the existing judicial backlog in India.[26] On the US side, some skeptics question whether any such agreement will meet the requirements in the CLOUD Act. Privacy and human rights groups in the US have criticised the CLOUD Act, overall, saying that its executive agreements would weaken existing privacy and other

protections.[27] These groups have also voiced more specific concerns about the first executive agreement, negotiated with the United Kingdom, and are awaiting an exchange of diplomatic notes to go into effect.[28] In response to these concerns, one of the authors of this report (Swire), with Prof. Jennifer Daskal of the American University Washington College of Law, has explained why a CLOUD Act executive agreement could improve privacy and other human rights protections.[29] The new research project on India-US data sharing must highlight not only the potential risks to fundamental rights that an executive agreement would bring, but more importantly, how those potential risks can be mitigated.

III. A POTENTIAL EXECUTIVE AGREEMENT: CRUCIAL ELEMENTS

The CBDF-ORF project seeks to identify the challenges facing India and the US should they enter into an executive agreement. It will explore means for overcoming such challenges.

The Role of the Judge in India

Under a CLOUD Act executive agreement, direct requests for content "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."[30] In India, however, it is common practice for a police officer to issue requests to service providers without any requisite judicial oversight. This lack of judicial participation could thus be found contrary to the CLOUD Act's provisions.

The 2019 ORF report suggested ways, consistent with current Indian law, whereby requests under an executive agreement could meet the judicial requirement.[31] Section 91 of the Indian Code of Criminal Procedure 1973 (CrPC)[32] provides two alternative routes to making a request for evidence:

1. A police officer can simply issue a written order to the person in possession of the relevant documents. This route is most often used by law enforcement agencies and is typically used without judicial approval.

2. Section 91 of the CrPC provides that a court may issue a summons ordering production of the relevant documents. According to the Indian Supreme Court, police officers can petition the court to compel the production of evidence "for the purpose of an investigation, inquiry, or trial."[33]

Potentially, only the second route would qualify under an India-US executive agreement. Without any need to change Indian law, investigators could choose the second route for direct requests to US service providers. Requests related to investigations that used the first route would not qualify for treatment under the executive agreement.

A similar analysis could apply to the CLOUD Act requirement that the order must be sufficiently "specific."[34] Section 93 of the CrPC permits search warrants which are of a general nature; however, the court may, "if it thinks fit," specify the particular places to which the warrant extends.[35] An Indian judicial warrant could thus qualify under the executive agreement only where the judge "thinks fit" to provide specificity.

Finally, the CLOUD Act requires that requests be "based on requirements for a reasonable justification based on articulable and credible facts."[36] Sections 91 and 93 CrPC do not require judges to expressly meet this particular standard, but for them to make a reasoned determination demonstrating application of mind (which is subject to judicial review by higher courts). Additionally, there is nothing in these sections to prevent a court from applying a higher standard as required by the CLOUD Act. In other words, current Indian law appears to authorise, but not mandate, a judge to issue a specific (not general) warrant based on facts that are credible and can be articulated. Such warrants would appear consistent with the CLOUD Act statutory requirements for the role of a judge.[37]

The approach proposed in this report, sets forth a general process that could reconcile the CLOUD Act requirements with Indian national law. Although 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 are expected elements under the CLOUD Act for an individual request for content. Under an 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. These procedural requirements, which are optional under Sections 91 and 93 CrPC, would be required for the request to qualify to be sent directly to a US service provider pursuant to an executive agreement between the two countries. Other Indian requests to a US service provider would not qualify, as is presently the case, for CLOUD Act treatment.

The Qualified Entity Approach

Other analyses have already addressed institutional structures that could enable administration within India of an executive agreement, consistent with the CLOUD Act.[38] Amongst the institutional requirements is the general one that the Indian government has "clear legal mandates and procedures governing those entities of the foreign government that are authorized 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."[39] The CLOUD Act also contains more specific institutional requirements, including, for example, the following:

- **Minimisation for US Personal Data.** The Indian government would have to implement "appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement."[40]

- **A Five-Year Compliance Review.** Every executive agreement is subject to a compliance review and renewal, at least once every five years.[41]

A potential approach to meet the institutional requirements needed so requests would qualify for treatment under the executive agreement is for the executive agreement to designate one or more "Qualified Entities." A "Qualified Entity" is an institution within India that provides the institutional safeguards outlined above. As discussed in the 2019 ORF/Georgia Tech report, this approach has the following potential advantages as compared with a general change in Indian law for criminal procedure:

- India can take the initiative in creating and defining the Qualified Entities. Compared with changing criminal procedure for all law enforcement for over a billion people, it would be more realistic for India to create and assign staff to one or a few offices in the government that meet statutory requirements for an executive agreement.

- The CLOUD Act contemplates institutional controls, transparency, compliance, and oversight for a Qualified Entity. One or a few Qualified Entities would be more affordable and manageable rather than applying institutional requirements to all Indian law enforcement requests.

- It is easier to authenticate requests from a Qualified Entity than from a multitude of different state and federal courts.

- Such Qualified Entities would also ensure that the CLOUD Act requirements are met for each individual request, such as that for having adequate specificity in a judicial order.

The 2019 report offered a proposal for a Qualified Entity within the Cyber and Information Security Division ("C&IS") of the Indian Ministry of Home Affairs ("MHA").[42] There are other possible institutional arrangements. The Qualified Entity could contain officers from state police agencies, to reflect the fact that policing is a state matter under the Indian Constitution. Under this approach, State police would not send requests to US service providers; instead, they would make direct requests to the service provider through an officer appointed to the Qualified Entity. More detailed work would be needed to define the institutional arrangements for Qualified Entities, and the new research project will do work in support of that effort.

Adherence to standards set by the Budapest Convention

The CLOUD Act lists requirements for adherence to the standards set by the Budapest Convention, the international treaty signed by more than 60 countries that governs cooperation on cybercrime.[43] To qualify for a CLOUD Act executive agreement, India must either become a party to the Budapest Convention, or have certain laws in place consistent with its Chapters I and II.[44] India would thus have two possible paths to comply with this part of the CLOUD Act.

First, India could become a party to the Budapest Convention. For years, there have been debates within India on whether or not to become a party to the treaty. News accounts have reported renewed interest by certain stakeholders to join the treaty, but others have put forward various reasons not to do so.[45] The new research project will report on these debates, assisting a well-informed discussion of this possibility.

With regard to the second path, Chapter I of the Budapest Convention requires that certain types of activities be criminalised, such as illegal access to computers, illegal interception, computer-related fraud, child pornography, and infringement of copyright. Chapter II contains procedural rules, such as expedited preservation of stored computer data, search and seizure of computer data, and real-time collection of traffic data. India has national laws that overlap considerably with the requirements of Chapters I and II. To explore the viability of this path, further research is necessary comparing the consistency of the requirements in the Budapest Convention and the relevant laws in India.[46]

Data Localisation

There is a significant possible tension between a CLOUD Act executive agreement and proposals in India for data localisation. To enter into an executive agreement, the CLOUD Act states that a foreign government must demonstrate "a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet."[47] Where India implements data localisation requirements, it arguably fails to meet this standard.

The original draft of the Indian Personal Data Protection Bill (PDP Bill) contained wide-ranging localisation obligations, imposing a requirement on "data fiduciaries" to store at least a copy of personal data in India (either exclusively or on mirror servers).[48] The most recent draft of the PDP Bill has slightly narrowed the localisation requirements, but they still would apply to "sensitive personal data" and "critical personal data."[49]

It is worth noting that law enforcement needs appear to have been one of the primary reasons behind the proposals for data localisation.[50] As explained earlier, under ECPA and the current MLAT system, law enforcement in India has difficulty ensuring timely access to content held by US service providers. Data localisation is seen as a method to enable law enforcement agencies to access such content data without resorting to the MLAT system, nor complying with foreign legal requirements such as having to demonstrate "probable cause."[51]

An executive agreement is a means to address these law enforcement concerns, without the need for data localisation.[52]

Areas for Future Research

The discussion thus far has highlighted four topics: the role of the judge; defining "qualified entities", the Budapest Convention, and data localisation. Beyond these four subjects, the work of CBDF and affiliated scholars has previously shown the substantial number of discrete issues that have required attention for CLOUD Act executive agreements generally, and more specifically, for US negotiations with the European Union, United Kingdom, and Australia.[53]

The new research project focused on India will similarly face a substantial number of additional issues. For instance, the US and India would need to define what constitutes a "serious crime," because the executive agreement

applies only to those crimes, and not more minor ones. The scope of an executive agreement can vary, and it is not clear whether and how an executive agreement would apply to real-time interception. Importantly, there are free speech and non-discrimination requirements in the CLOUD Act. Additional research may therefore be needed to clarify the law and practice in India, and explore ways to proceed that could meet these human rights requirements in the Act.

CONCLUSION

An India-US executive agreement could have substantial benefits, such as fulfilling legitimate law enforcement requests, thereby alleviating a primary driver for data localisation and providing new protections within India for privacy and human rights. Substantial research and discussion will be needed to identify and refine possible solutions for the legal issues arising from a India-U.S. executive agreement under the CLOUD Act.

Moreover, such an agreement can only succeed if the ultimate agreement is acceptable to the political leaders of the two countries. The CBDF-ORF research project aims to provide an informed basis for the formulation of responses to the important issues related to the Indian government's access to evidence held in the US. ORF

(The views expressed in this report are those of the authors and do not reflect the official position of the Cross-Border Data Forum, the Observer Research Foundation, or any member or affiliate organisations.)

About the Authors

Peter Swire is the Elizabeth and Tommy Holder Chair and Professor of Law and Ethics in the Scheller College of Business at the Georgia Institute of Technology, and is senior counsel with the law firm of Alston & Bird. **DeBrae Kennedy-Mayo** is a Research Faculty Member at the Scheller College of Business at the Georgia Institute of Technology. **Arjun Jayakumar** is an Associate Fellow at ORF's Cyber Initiative.

ENDNOTES

1 In 2018, the United States enacted the Clarifying Lawful Overseas Use of Data Act: Consolidated Appropriations Act, 2018, P.L. 115-141, div. V ("CLOUD Act"). *See* 18 U.S.C. 2523, https://www.law.cornell.edu/uscode/text/18/2523.

2 The 2019 report was authored by three faculty members from the Georgia Institute of Technology – Peter Swire, DeBrae Kennedy-Mayo, and Sreenidhi Srinivasan – and one ORF researcher – Madhulika Srikumar. *See* DeBrae Kennedy-Mayo, Peter Swire, Sreenidhi Srinivasan and Madhulika Srikumar, "India-U.S. Data Sharing for Law Enforcement: Blueprint for Reforms," Observer Research Foundation, January 17, 2019, https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf.

3 These goals are stated on the Cross-Border Data Forum website, www.crossborderdataforum.org.

4 Manish Singh, "Indian Startups Diversify Their Businesses to Offset COVID-19 Induced Losses," *TechCrunch*, June 29, 2020, https://techcrunch.com/2020/06/28/indian-startups-diversify-their-businesses-to-offset-covid-19-induced-losses/; Manish Singh, "Amazon Temporarily Discontinues 'Lower Priority' Items; Flipkart Suspends All New Orders," *TechCrunch*, March 24, 2020, https://techcrunch.com/2020/03/24/amazon-prioritizes-essential-products-in-india-temporarily-discontinues-lower-priority-items/.

5 "De-Globalisation, A Business Truth in Post-Pandemic World: Survey," *The Hindu*, May 12, 2020, https://www.thehindu.com/business/de-globalisation-a-business-truth-in-post-pandemic-world-survey/article31566127.ece; Shivaji Bhattacharya & Anindhya Shrivastava, "India: COVID-19: Implications on the Data Protection Framework in India," *Mondaq*, May 6, 2020, https://www.mondaq.com/india/data-protection/928998/covid-19-implications-on-the-data-protection-framework-in-india; *see* Kirtika Suneja, "E-Commerce Policy Put On Hold," *The Economic Times*, May 12, 2020, https://economictimes.indiatimes.com/news/economy/policy/e-commerce-policy-put-on-hold/articleshow/75683719.cms.

6 ECPA is a federal law in the U.S. governing interception of communications in transit as well as access to stored data by law enforcement. The discussion in this paper focuses on Title II of ECPA – called the Stored Communications Act (SCA) – which details protections for the contents of communications stored with service providers as well as the records held about the subscriber by the service providers. *See* 18 U.S.C. 2701-2712, https://www.law.cornell.edu/uscode/text/18/2701. For an overview of ECPA, view "Electronic Communications Privacy Act of 1986 (ECPA)," Privacy & Civil Liberties, Justice Information Sharing, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

7 Law Enforcement Mutual Legal Assistance, Treaty between the United States of America and India, October 17, 2001, https://www.state.gov/wp-content/uploads/2019/02/05-1003-India-Mutual-Legal-Assist-Treaty.pdf.

8 Jennifer Daskal, Peter Swire, and Theodore Christakis, "The Globalization of Criminal Evidence," IAPP, October 16, 2018, https://iapp.org/news/a/the-globalization-of-criminal-evidence/; *see also* Peter Swire, "Why Cross-Border Government Requests for Data Will Keep Becoming More Important," Lawfare, May 23, 2017, https://www.lawfareblog.com/why-cross-border-government-requests-data-will-keep-becoming-more-important.

9 DeBrae Kennedy-Mayo, Peter Swire, Sreenidhi Srinivasan and Madhulika Srikumar, "India-U.S. Data Sharing for Law Enforcement: Blueprint for Reforms," Observer Research Foundation, p. 8, January 17, 2019, https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf.

10 *See* 18 U.S.C. 2703, https://www.law.cornell.edu/uscode/text/18/2703.

11 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. Within the U.S., there are legal rules that require U.S. 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 so, service providers can voluntarily disclose customer records and subscriber information to "any person other than a US government entity." 18 U.S.C. 2702(c)(6), https://www.law.cornell.edu/uscode/text/18/2702. This enables service providers to disclose certain non-content data to non-U.S. government or law enforcement agencies.

12 The "probable cause" standard is often unfamiliar to those outside the U.S. In defining the "probable cause" standard, the U.S. 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." *See* Illinois v. Gates, 462 U.S. 213, 238 (1983).

13 The widely influential 6th Circuit case of *United States v. Warshak* 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." *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), https://www.opn.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf. Observers have expressed their opinion that there is a strong likelihood that the *Warshak* approach would be adopted if the U.S. Supreme Court were to review the topic. Note that U.S. service providers may also 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.

14 DeBrae Kennedy-Mayo, Peter Swire, Sreenidhi Srinivasan and Madhulika Srikumar, "India-US Data Sharing for Law Enforcement: Blueprint for Reforms," Observer Research Foundation, p. 59, January 17, 2019, https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf; *see* Peter Swire & Justin Hemmings, "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program," 71 NYU Annual Survey of American Law 687, 696 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728478; Jennifer Daskal & Andrew Woods, "Cross-Border Data Requests: A Proposed Framework," Lawfare, November 24, 2015, https://www.lawfareblog.com/cross-border-data-requests-proposed-framework.

15 For example, the Facebook transparency report for the last half of 2019 states that Indian law enforcement received some data from the company for 57% of submitted requests; similarly, Google reports that 62% of Indian requests received some data for the same time period. Government Requests for User Data – India, Facebook Transparency Report (2019), https://transparency.facebook.com/government-data-requests; Requests for User Information, Google Transparency Report (2019), https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts;authority:DE;time:Y2019H2&lu=user_requests_report_period. It may be noted here that requests made by U.S. law enforcement to service providers also sometimes do not responsive documents. Scholars have emphasised the need for enhancing training at all levels of law enforcement within the U.S. *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.

16 This statistic is a 2013 estimated average for all requests from all countries, and no statistics related to specific countries were 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.

17 A 2015 article estimated an average delay of 40 months for Indian law enforcement agencies to receive electronic evidence for a U.S. service provider. Neha Alawadhi, "CBI & FBI Join Hands to Reduce Time Required to Fulfil Requests on Information and Evidence," *The Economic Times*, December 7, 2015, https://economictimes.indiatimes.com/news/politics-and-nation/cbi-fbi-join-handsto-reduce-time-required-to-fulfil-requests-on-information-and-evidence/articleshow/50069794.cms.

18 At the time of the writing of this article, the population of India was approximately 1.4 billion people. India Population 2020, World Population Review, http://worldpopulationreview.com/countries/india-population/. India has nearly 700 million Internet users. Internet Usage in India – Statistics and Facts. Statista, https://www.statista.com/topics/2157/internet-usage-in-india/. In the last half of 2019, Facebook received 26,698 requests from India, and Google received 10,891. Government Requests for User Data – India, Facebook Transparency Report (2019), https://transparency.facebook.com/government-data-requests; Requests for User Information – India, Google Transparency Report (2019), https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts;authority:IN;time:&lu=user_requests_report_period. The traditional treatment of requests through treaty mechanisms was never designed for this scale of potential cases.

19 For example, Facebook received the greatest number of foreign requests in the last half of 2019 from India, with a total of 26,698 requests. During this timeframe, Facebook received the second highest number of requests from Germany, with Germany law enforcement making 8,013 requests. Government Requests for User Data, Facebook Transparency Report (2019), https://transparency.facebook.com/government-data-requests. For the last half of 2019, Google received the most foreign requests from Germany, with a total of 11,160. Google received the second highest number of requests from India, with Indian law enforcement making 10,891 requests. Requests for User Information, Google Transparency Report (2019), https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts;authority:DE;time:Y2019H2&lu=user_requests_report_period. To put the number of requests from these two countries into context, India has a population of approximately 1.4 billion, while Germany's population is approximately 84 million. World Population Review, https://worldpopulationreview.com/countries.

20 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 U.S.). 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.

21 Under the executive agreement between the two countries, the U.S. could agree to allow direct access to U.S. service providers when certain requirements were met. This approach should lessen the number of requests being made through the MLAT process.

22 18 U.S.C. 2523(b)(1)(B)(iv) (emphasis supplied), https://www.law.cornell.edu/uscode/text/18/2523.

23 18 U.S.C. 2523(b)(2), https://www.law.cornell.edu/uscode/text/18/2523.

24 18 U.S.C. 2523(b)(4)(D), https://www.law.cornell.edu/uscode/text/18/2523.

25 18 U.S.C. 2523(b)(4)(D)(v), https://www.law.cornell.edu/uscode/text/18/2523.

26 DeBrae Kennedy-Mayo, Peter Swire, Sreenidhi Srinivasan and Madhulika Srikumar, "India-US data sharing for law enforcement: Blueprint for reforms," Observer Research Foundation, p. 65-67, January 17, 2019, https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf.

27 ACLU, Coalition Letter on CLOUD Act, https://www.aclu.org/letter/coalition-letter-cloud-act.

28 Paul Greaves & Peter Swire, "New Developments for the U.K. and Australian Executive Agreements With the U.S. Under the CLOUD Act," Cross-Border Data Forum, 19 July 2020, https://www.crossborderdataforum.org/new-developments-for-the-u-k-and-australian-executive-agreements-with-the-u-s-under-the-cloud-act-2/; *see* Joe Mullin, "U.K. Police Will Soon Be Able to Search Through U.S. Data Without Asking a Judge," EFF, January 29, 2020, https://www.eff.org/deeplinks/2020/01/uk-police-will-soon-be-able-search-through-us-data-without-asking-judge.

29 Jennifer Daskal & Peter Swire, "The U.K.-U.S. CLOUD Act Agreement is Finally Here, Containing New Safeguards," Lawfare, Oct. 8, 2019, https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards; Jennifer Daskal & Peter Swire, "Privacy and Civil Liberties Under the CLOUD Act: A Response," Lawfare, March 21, 2018, https://www.lawfareblog.com/privacy-and-civil-liberties-under-cloud-act-response.

30 18 U.S.C. 2523(b)(4)(D)(v), https://www.law.cornell.edu/uscode/text/18/2523.

31 DeBrae Kennedy-Mayo, Peter Swire, Sreenidhi Srinivasan and Madhulika Srikumar, "India-US Data Sharing for Law Enforcement: Blueprint for Reforms," Observer Research Foundation, p. 34-35, January 17, 2019, https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf.

32 Indian Criminal Procedure Code, S.91, https://indiankanoon.org/doc/788840/.

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

34 The CLOUD Act provides that the request "shall identify a specific person, account, address, or personal device, or any other specific identifier as the

object of the order." 18 U.S.C. 2523(b)(4)(D)(ii), https://www.law.cornell.edu/uscode/text/18/2523.

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

36 18 U.S.C. 2523 (b)(4)(D)(iv), https://www.law.cornell.edu/uscode/text/18/2523.

37 Under this analysis, current Indian procedures could continue for investigations that do not seek access to content under the executive agreement. One privacy advantage of the proposed approach is that Indian judges and police would gain experience with the stricter procedural protections required for requests under the executive agreement.

38 DeBrae Kennedy-Mayo, Peter Swire, Sreenidhi Srinivasan and Madhulika Srikumar, "India-US Data Sharing for Law Enforcement: Blueprint for Reforms," Observer Research Foundation, p. 60-63, January 17, 2019, https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf,; *see also* Peter Swire & Deven Desai, "A 'Qualified SPOC' Approach for India and Mutual Legal Assistance," Lawfare, March 2, 2017, https://www.lawfareblog.com/qualified-spoc-approach-india-and-mutual-legal-assistance. In that article "SPOC" stands for "single point of contact."

39 18 U.S.C. 2523(b)(1)(B)(iv), https://www.law.cornell.edu/uscode/text/18/2523.

40 18 U.S.C. 2523(b)(2), https://www.law.cornell.edu/uscode/text/18/2523. The term "appropriate procedures" is not defined in the statute.

41 18 U.S.C. 2523(b)(4)(J) & (e)(1), https://www.law.cornell.edu/uscode/text/18/2523.

42 The report noted that 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 this article. *See* DeBrae Kennedy-Mayo, Peter Swire, Sreenidhi Srinivasan and Madhulika Srikumar, "India-US Data Sharing for Law Enforcement: Blueprint for Reforms," Observer Research Foundation, p. 61-63, January 17, 2019, https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf

43 Convention on Cybercrime, European Treaty Series - No. 185, Council of Europe, November 23, 2001, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf; *see* Chart of Signatures and Ratifications of Treaty 185, Convention on Cybercrime, Treaty Office, Council of Europe (status as of October 2020), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

44 18 U.S.C. 2523(b)(1)(B)(i), https://www.law.cornell.edu/uscode/

text/18/2523. Chapters I and II of the Budapest Convention describe measures to be taken at the country level regarding both substantive law and procedural law. Convention on Cybercrime, European Treaty Series - No. 185, Council of Europe, November 23, 2001, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

45 See, for example, Alexander Seger, "India and the Budapest Convention: Why Not?," Observer Research Foundation, October 20, 2016, https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/.

46 See, for example, Vipul Kharbanda, "Budapest Convention and the Information Technology Act," The Centre for Internet & Society, November 20, 2018, https://cis-india.org/internet-governance/blog/budapest-convention-and-the-information-technology-act.

47 18 U.S.C. 2523 (b)(1)(B)(vi), https://www.law.cornell.edu/uscode/text/18/2523.

48 The Personal Data Protection Bill, 2018, https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians," July 27, 2018, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

49 The 2019 Bill narrows the data localisation requirement to mirroring of sensitive personal data and processing of critical personal data only in India (subject to exceptions). Practically speaking, this means an intermediary would have to review all data to make a determination if it is personal or sensitive or critical personal data and could possibly lead to over compliance by localisation of all data. *See* Kurt Wimmer and Gabe Maldoff, "India Proposes Updated Personal Data Protection Bill," Inside Privacy, Covington & Burlington, December 12, 2019, https://www.insideprivacy.com/india/india-proposes-updated-personal-data-protection-bill/. India delayed review of the 2019 Bill due to the COVID-19 pandemic. "India's Personal Data Protection Bill," OneTrust, July 24, 2020, https://www.onetrust.com/indiias-personal-data-protection-bill/.

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

51 Jennifer Daskal & Peter Swire, "Why the CLOUD Act is Good for Privacy and Human Rights," Lawfare, March 14, 2018, https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights.

52 DeBrae Kennedy-Mayo, Peter Swire, Sreenidhi Srinivasan and Madhulika Srikumar, "India-U.S. Data Sharing for Law Enforcement: Blueprint for Reforms," Observer Research Foundation, p. 53, January 17, 2019, https://

www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf.

53 Justin Hemmings, Sreenidhi Srinivasan and Peter Swire, "Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the CLOUD Act," Cross-Border Data Forum, November 6, 2019, https://www.crossborderdataforum.org/defining-the-scope-of-possession-custody-or-control-for-privacy-issues-and-the-cloud-act/; Peter Swire & Jennifer Daskal, "Frequently Asked Questions about the U.S. CLOUD Act," Cross-Border Data Forum, April 16, 2019, https://www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act; *see* Jennifer Daskal, "Correcting the Record: Wiretaps, the CLOUD Act, and the US-UK Agreement," Just Security, October 31, 2019, https://www.justsecurity.org/66774/correcting-the-record-wiretaps-the-cloud-act-and-the-us-uk-agreement/; Peter Swire, "Comments on Australian Legislation to Enable the Negotiation of a U.S. CLOUD Act Executive Agreement," Cross-Border Data Forum, May 11, 2020, https://www.crossborderdataforum.org/comments-on-australian-legislation-to-enable-the-negotiation-of-a-u-s-cloud-act-executive-agreement/.

Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. Fax : +91-11-35332005.
E-mail: contactus@orfonline.org
Website: www.orfonline.org