CARNEGIE INDIA

WORKING PAPER

NOVEMBER 2020

Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?

Smriti Parsheera and Prateek Jha

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?

Smriti Parsheera and Prateek Jha

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, D.C. 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

Carnegie India
Unit C-5 & C-6, Edenpark,
Shaheed Jeet Singh Marg
New Delhi - 110016, India
P: + 011 4008687
CarnegieIndia.org

This publication can be downloaded at no cost at CarnegieIndia.org.

CONTENTS

Summary

Access to cross-border data for the state's law-and-order-related functions is an integral piece of the law enforcement puzzle. State agencies' ability to access data for such purposes is, however, shaped not only by domestic laws and practices but also by the laws of other countries and the state's international commitments. In the case of India, the use of international cooperation mechanisms to balance efficient data access with protections for citizens' privacy remains a relatively underexplored facet of its digital strategy. With its growing digital market, economic relevance for large global businesses, and strategic relationships with countries like the United States and those in the European Union (EU), India is well placed to not merely participate in but rather to lead the discussions on international data agreements on behalf of the developing world.

This paper evaluates India's present mechanisms for data access by law enforcement authorities and existing arrangements for cross-border data access. It also analyzes the emerging global movement toward direct data access arrangements. Such arrangements authorize agencies in one jurisdiction to make direct data requests to service providers based in another jurisdiction. The Clarifying Lawful Overseas Use of Data (CLOUD) Act in the United States is an example of a legislative instrument that allows the United States to enter into executive agreements of this nature. Similar discussions are also underway in Europe under the European Commission's e-evidence proposal involving its twenty-seven member countries and among the sixty-five states that are party to the Budapest Convention on Cyber Crimes. To date, India has not taken any concrete steps to evaluate the pros and cons of such arrangements. Neither has it paid serious regard to the critical and interconnected issue of reforming its domestic framework on lawful data access to ensure adherence with the fundamental right to privacy.

To address these issues, India should take several steps. First, it should revisit its domestic legal framework on lawful data access to incorporate necessary proportionality standards and procedural safeguards as soon as possible. Suggestions for improvements include the need for prior authorization of access requests by a judicial or other independent body, oversight of data processing activities, transparency and reporting requirements, notice to affected individuals, and application of other data protection principles. These reforms are important not just from the perspective of ensuring adherence to the tests laid down by the Supreme Court of India while affirming the fundamental right to privacy, but also as a means of signaling India's suitability as a potential negotiating partner for any international arrangements on direct data access. This link between a country's domestic surveillance framework and the validity of its international data access and transfer commitments has become all the more relevant in light of the European court's decision in the *Schrems II* case.[1]

Second, India should evaluate the substantive and procedural reforms needed to its cross-border access arrangements. At present, mutual legal assistance treaties (MLATs) remain the dominant international framework for enabling cross-border data access. These treaties, however, have shown only limited functionality in dealing with the volume and expected speed of compliance of present-day data requests. This gives rise to a need for structural reforms in the MLAT framework. India's strategies on cross-border data access must also be informed by the global developments around data access. Of particular note is the ongoing shift in the international mood toward direct access arrangements. These arrangements are being seen as alternatives to the MLAT processes, at least in terms of data requests pertaining to serious crimes and those that require immediate action.

India will need to develop a strategic position on the adoption of direct access arrangements. Instead of treating the CLOUD Act or any other available model as a fait accompli, India should develop its own model international agreement on direct access to data. Doing so would ensure that any future negotiations on the subject will not be shaped solely by the positions set forth by potential counterparties. Given the complexity of issues at play here, spanning across domains of international relations, law enforcement, and civil liberties, the task of formulating India's position on this subject should not be left to the discretion of executive negotiations.

Accordingly, the Indian government should convene a task force with a diverse group of stakeholders—including representatives from different government departments, the private sector, civil society organizations, researchers, and experts in international law—to formulate India's model data transfer agreement through an open and consultative process. This model agreement may be informed by suitable elements from the CLOUD Act, the EU's e-evidence proposal, and the Second Additional Protocol to the Budapest Convention, and yet it should ultimately signal India's unique negotiating position and a commitment to the highest standards of data protection. This paper makes some recommendations on what may be regarded as the key elements of the proposed model agreement.

Third, India should work toward creating a streamlined mechanism to transmit, authenticate, and complete the direct data requests being made to service providers. Such a mechanism will help build legitimacy and trust in the process for lawful data access. This would be relevant both for existing data access requests as well as any new arrangements that may be adopted pursuant to international agreements. Suggested features of this new system include appropriate authentication protocols and access controls mechanisms, standardized request formats, encryption protocols for secure data transmission, and maintenance of access logs. Standard operating procedures and training modules will help ensure that the proposed policies and systems actually result in improved implementation outcomes.

A multipronged strategy along all these fronts would help in building a protocol that achieves more efficient access to cross-border data within the contours of a rights-respecting framework.

Introduction

The average internet user in India consumes about 10.40 gigabytes (GB) of wireless data per month on communications, entertainment, information and a host of other online services.[2] As personal and commercial interactions increasingly move to the digital space, the state's interest in gaining better knowledge about these transactions has also increased. More detailed information about such transactions may help a state design better policy interventions, monitor regulatory compliance, and discharge its law enforcement functions more effectively.[3] This paper focuses on the last category of data access—namely, data required in connection with the state's law-and-order functions.

State agencies' ability to gain access to data for law enforcement purposes is shaped to a significant extent by the cross-border character of digital transactions. This includes situations where the entity in control of the data or the location of the stored data may be based outside the country. Per the European Commission's estimates, electronic evidence is needed in around 85 percent of criminal investigations, two-thirds of which involve online service providers based in another jurisdiction.[4] Similar figures are not available for India, but transparency reports released by service providers offer a valuable indicator of the growing digital footprint of criminal investigations. For instance, Facebook received 49,382 information requests from India in 2019, three times higher than the request volume in 2016.[5] Similar trends have been seen in transparency reports from Google and Twitter.[6] This trend may be attributed, in part, to the sharp rise in India's internet user base in the last three to four years.[7] This explosive rise has led to a corresponding increase in the volume of digital transactions, many of which tend to have cross-border elements.

Cross-border data access requests are governed both by the local laws of the country making the request, and those of the jurisdiction where the entity receiving the request or its data storage facility is based. Often, these laws may limit personal data access by third parties, including foreign government agencies. The normal route to gain access to data under such circumstances is through the use of MLATs (mutual legal assistance treaties). As of November 2019, India had entered into MLATs with forty-two countries and was a signatory to six international conventions with mutual legal assistance provisions.[8] However, the MLAT route remains widely criticized for being slow and cumbersome and lacking sufficient data protection safeguards.[9] As a result, policymakers have sought other alternative models of data access for law enforcement purposes, making it a recurring theme in many policy discussions.

Access to data for crime detection and evidence gathering was a rationale given by the Justice B. N. Srikrishna Committee on data protection while proposing the localization of personal data in India.[10] Following the findings of that committee's report, the government introduced a draft Personal Data

Protection Bill (PDP Bill) in 2019, which provided for local storage only for sensitive data but local storage and processing for more critical types of personal data.[11] The draft intermediary guidelines, which have been in the pipeline for about two years, are another attempt to make intermediaries more responsive to law enforcement requests. For instance, the draft rules require intermediaries to furnish a prompt response to information requests (within seventy-two hours) and mandate a local incorporation requirement for intermediaries above a certain size, which is presumably meant to ensure better enforcement.[12] Most recently, the Kris Gopalakrishnan Committee on nonpersonal data has spoken about simplifying access to data for national security, law enforcement, legal, and regulatory purposes.

Measures such as data localization and other intrusive mechanisms for securing unfettered government access to data can have worrying implications for individual liberties and business freedoms. For instance, mandates to use local storage may limit providers from choosing the most efficient and viable data storage arrangements. At the same time, local storage requirements expose individuals to a greater threat of unchecked surveillance by domestic agencies.[13] The discussions on government data access are, therefore, closely intertwined with the need for greater transparency, oversight, and accountability in the government's ability to access citizens' personal data. A rethinking of the Indian legal framework on these counts has become particularly necessary in light of the Supreme Court's verdict in the *Justice K. S. Puttaswamy* v. *Union of India* case, which recognized privacy to be a fundamental right.[14]

Recent global developments highlight the link between a country's surveillance framework and the level of trust that other jurisdictions or businesses may place in its systems. One of the grounds for the invalidation of the Privacy Shield by the EU Court of Justice in the *Schrems II* case was that the U.S. surveillance architecture contradicts the privacy rights of EU citizens under their own laws.[15] The reluctance shown by technology companies to share data with Hong Kong authorities, in the wake of the broad powers conferred under a new national security law, is another case in point.[16] All of these developments point toward the need to build efficacious solutions for data access that also respect users' privacy.

With this objective in mind, this paper examines two interrelated question sets. First, how can India's laws and practices on data access for law enforcement purposes be improved in line with the constitutional right to privacy? Second, what kind of bilateral or multilateral arrangements on data access should India consider to improve cross-border access, and what could be the key elements of such arrangements?

To develop feasible responses to these questions, the authors conducted interviews with government, civil society, and industry stakeholders, and held discussions at a roundtable on this subject at the Carnegie India Global Technology Summit in 2019. The paper also draws upon the existing literature on three key points—necessary reforms to India's state surveillance architecture;[17] challenges with the MLAT processes and other existing modes of data access;[18] and evaluation of the CLOUD Act's compatibility with India's laws and practices.[19]

Following this introduction, the second section presents an outline of India's legal framework on lawful data access, the challenges with the present system, and the authors' suggested reforms. The third section follows a similar pattern of presenting the present status, challenges, and recommendations pertaining to different mechanisms for cross-border data access. Key mechanisms considered include MLATs, letters rogatory (LR), and provision of direct access to certain kinds of data offered by various service providers. The fourth section examines the ongoing moves toward adoption of bilateral and multilateral arrangements to facilitate direct data access. These arrangements seek to authorize authorities in one jurisdiction to directly call for information from service providers based in another jurisdiction. It discusses the status, key provisions, and concerns raised by such arrangements. The fifth section sets out the authors' recommendations on the next steps for formulating India's strategic position on direct data access agreements and some of the suggested components of such agreements. Finally, the conclusion summarizes the recommended improvements to India's present laws and practices, and discusses the next steps needed to strengthen its international arrangements for cross-border data access.

Domestic Legal Framework on Data Access

A sound legal framework on access to data by local law enforcement agencies is critical for building trust among citizens, service providers, and civil society. In order to achieve this in the Indian legal context, the domestic framework should ensure adherence to the fundamental right to privacy. Such adherence can also act as a signal of India's suitability as a potential partner for any international arrangements on cross-border data access.

Police authorities in India most commonly rely on section 91 of the Criminal Procedure Code (CrPC) to access any "document or other thing" that may be required in the course of an investigation. The provision creates two routes for enabling access to information: through a summons issued by a court or pursuant to a written order issued by the officer in charge of a police station. Addition-

ally, the police and other investigative agencies have the power to seek the interception or disclosure of a message or information on a computer resource under the Indian Telegraph Act, 1885 and the Information Technology Act, 2000 (IT Act).[20] Of these, the Telegraph Act, despite its earlier vintage, provides a slightly higher legal threshold for seeking access to data.[21] In a December 2018 order, the government listed ten investigation and security agencies that are authorized to issue interception, monitoring, and decryption requests under the IT Act.[22] This list includes bodies such as the Intelligence Bureau, Narcotics Bureau, and Enforcement Directorate.

The ongoing process toward the adoption of a comprehensive data protection law also bears significant implications for domestic data access. The draft PDP Bill introduced in the Parliament of India in December 2019 contains widely worded exemptions for law enforcement purposes. Notably, section 35 of the bill allows for agency-based exemptions from any or all provisions of the bill on certain grounds.[23] Further, section 36(1)(a) of the bill exempts any data processing carried out for the "prevention, detection, investigation, and prosecution of any offence or any other contravention of any law for the time being in force" from most of the substantive requirements under the law. By failing to restrict its scope only to offenses under, or contravention of, Indian laws, section 36(1)(a) creates some ambiguity around the possibility of its use for enabling the transfer of user data for foreign law enforcement purposes. This ambiguity becomes particularly relevant given that the few identified provisions of the law that would still be applicable in such circumstances do not include the restrictions on cross-border data transfers that appear in chapter VII of the PDP Bill.

Challenges of the Present System

Notably, neither the general criminal law nor the telecom and information technology sector-specific laws mandate the need for judicial approval before allowing access to users' information.[24] In 1997, the Supreme Court observed, in the context of a phone-tapping case, that "in the absence of any provision in the statute, it is not possible to provide for prior judicial scrutiny as a procedural safeguard."[25] The court then went on to suggest an administrative oversight mechanism in which each data request would have to be approved by the home secretary, or in some cases a joint secretary in the central or relevant state government. This mechanism has now become the accepted legal process under the rules adopted under both the Telegraph Act and the IT Act.

The insufficiency of these mechanisms, however, becomes apparent when considering the volume of data access requests being approved by the designated officials. A right to information request made by the Software Freedom Law Center a few years back had revealed that the central government

alone was issuing an average of around 7,500 to 9,000 telephone interception orders each month.[26] This figure is significant in itself, but it represents only a fraction of the total number of data requests in the system.

Besides the lack of sufficient oversight, the present laws have also been criticized for being overly broad in terms of the scope of the powers and silent on necessary restrictions and limitations.[27] Some specific concerns include the absence of reporting and transparency requirements, insufficient internal checks, action with no notice to the individual, and lack of redress mechanisms.[28] In some cases, basic requirements may exist on paper, but with a significant gap between the stated rules and outcomes. For instance, even though there are rules that require a paper trail for every interception request, minimal information is available in the public domain to verify its implementation.[29]

Absence of adequate checks often leads to situations of unauthorized access and misuse by frontline officials. For instance, in 2013, news reports revealed that 1,371 phones had been tapped in the state of Himachal Pradesh by the Criminal Investigation Department and the Vigilance Bureau although the state's home secretary had authorized the interception of only 171.[30] Another example of misuse was seen when a police constable was able to use the official email address of a senior official to gain access to the call detail records of a prominent political leader.[31]

With the emphatic recognition of the fundamental right to privacy in the *Puttaswamy* case, the state's surveillance powers are once again being challenged before the Supreme Court.[32] The pending challenges seek to test the surveillance framework created under the IT Act and the Telegraph Act against the principles laid down by the Supreme Court in its nine-judge bench decision. The Supreme Court held that any infringement of the right to privacy by the state would be valid only if it is lawful, seeks to serve a legitimate aim, and is proportionate in nature.[33] Of these, the state might find it easier to argue for the satisfaction of the first two tests: the role of law enforcement as a legitimate state function is well recognized, and certain legal provisions (though broadly worded) enable data access by law enforcement authorities. However, in the absence of prior judicial review or other forms of effective independent oversight over investigation processes and lack of other reasonable safeguards, the current legal framework falls short of satisfying the requirements of proportionality. The widely worded exemptions for law enforcement agencies and purposes under the PDP Bill are likely to perpetuate these concerns.

Recommended Approach

The inadequacies of the present legal framework on lawful data access ideally should be addressed by introducing comprehensive legislation governing the functioning of intelligence and law enforcement agencies. However, pending that decision, the legislature should in any case revisit the existing provisions on lawful access under the CrPC, the Telegraph Act, and the IT Act. The objective of the legal changes should be to bring about appropriate checks and balances in the functioning of current data access mechanisms, broadly in line with the "Necessary and Proportionate" principles formulated by a coalition of civil society organizations.[34]

In the Indian context, some of the suggested legal requirements would be as follows:[35]

1. Prior judicial authorization or approval by an independent body of any data access requests for law enforcement purposes.

2. Oversight of surveillance activities by a parliamentary committee. The existing framework of department-related Parliamentary Standing Committees can be leveraged for this purpose. This task could be entrusted to either the Standing Committee on Information Technology or the Standing Committee on Home Affairs.

3. Notice to the affected individuals, which may be deferred with authorization of the independent approving authority, if earlier notice might jeopardize the investigation or proceedings.

4. Application of data protection principles like data minimization, data safety and security, destruction after use, and restrictions on interdepartmental sharing without specific authorization.

5. Appointment of privacy or data protection officers within each law enforcement agency to be responsible for ensuring compliance with the data protection norms.

6. Transparency and reporting requirements in relation to the number and nature of data requests being made. Along with the public reporting of figures by the relevant law enforcement agencies, the National Crime Records Bureau could be tasked with the responsibility of compiling the statistics on state and agency level data requests.

To the extent that any sort of surveillance reforms are sought to be achieved through the PDP Bill, it becomes necessary that any exceptions granted to law enforcement agencies should be narrowly tailored. In particular, the scope of the exemptions should be limited only to processing that which is

being done in the context of serious offenses under Indian laws. Such offenses may, for instance, be defined to mean those punishable by at least five years' imprisonment.[36] Further, the exemption provision should not exclude the application of some of the basic protections under the PDP Bill, such as requirements for fair and reasonable data processing (section 5), collection limitation (section 6), and restrictions on data retention (section 9).[37]

At the same time, the manner in which the PDP Bill intends to deal with cross-border data requests from foreign law enforcement agencies needs to be clarified. According to the structure of the bill, any data transfer that is otherwise not exempted under a specific provision ordinarily would require the individual's prior consent. Relying on consent may, however, not be a feasible option for entertaining data requests from foreign law enforcement agencies. Such requests also may not fall under any of the permissible grounds for processing without consent. Such grounds include compliance with any law made by the Indian Parliament or a state legislature or compliance with the orders of an Indian court.[38] Therefore, even in bilateral or multilateral agreement-based data access, service providers governed by the PDP Bill may require an authorizing law or an order from an Indian court to transfer data abroad without the individual's consent. The contours of such international arrangements should, therefore, be discussed along with the conversations on the PDP Bill.

Existing Mechanisms for Cross-Border Data Access

Law enforcement agencies typically request data that fall under three broad heads. The first is *basic subscriber information*, such as name, age, address, and other details that the subscriber provides at the time of enrollment. The second is *traffic* or *metadata*, including the origin, destination, time, and duration of the communication. The third involves the underlying *content* of the communication, which could be in a stored form or may entail the interception of live communications. On receiving a valid request under Indian law, ordinarily the responding entity is required to provide the requested information from any of these categories. However, in practice, domestic law enforcement agencies have varied ability to gain access to the data, depending on the nature of the information requested, the location of the service provider or the data storage facility, and the laws governing each of these aspects. Other factors, like data encryption, can also affect authorities' ability to access certain kinds of data.

According to the United States' Stored Communications Act, entities that fall within its jurisdiction are barred from sharing the contents of stored communication, except in accordance with the provisions of that law.[39] One of the permissible forms of access is through a court order passed in the United States, if the requesting entity can demonstrate that there are "reasonable grounds to believe"

that the contents being sought are relevant for an ongoing investigation.[40] Law enforcement agencies in India may also take advantage of this option by asking their U.S. counterparts to seek a court order for access to data pursuant to the terms of the MLAT between the two countries.[41] U.S. law also permits service providers to share non-content-related records or other information pertaining to a subscriber with foreign agencies on a voluntary basis.[42]

Another available access route is to seek information through the LR process. An LR is a formal request issued by a criminal court in India, at the request of an investigating agency, seeking the assistance of a court or authority in another jurisdiction for gathering evidence.[43] This process is often used in situations where there is no MLAT between the parties or the information being sought falls outside the scope of the treaty. In addition, an LR can be issued to any other country without a bilateral or multilateral arrangement, based on an assurance of reciprocity.

In addition, India is also a member of the G7 (Group of 7) 24/7 Cybercrime Network.[44] This network of about eighty countries was formed "to enhance and supplement (but not replace) traditional methods of obtaining assistance" by enabling the preservation of electronic evidence in other participating countries.[45] Its genesis lies in the recognition that delays in being able to obtain access to evidence held in another jurisdiction could result in the loss or destruction of the electronic evidence. To address this concern, each member of the network agrees to designate a twenty-four-hour point of contact for handling preservation requests and to make best efforts to get internet service providers to freeze the information that may be required for law enforcement purposes.[46] This mechanism, however, focuses only on the preservation of information and not its production, so countries still must rely on MLATs or LR for that purpose.[47]

Challenges of the Present System

Despite the availability of these different mechanisms, law enforcement agencies in India have reported practical difficulties in gaining access to data in a cross-border context. The first issue relates to delays in gaining access to the required information under the MLAT/LR route. As described above, the process of obtaining data through the MLAT route can be complex, involving multiple agencies in both countries. The LR process, similarly cumbersome, can be even slower than the MLAT route.[48] As per a 2013 report prepared by the U.S. President's Review Group on Intelligence and Communications Technologies, Liberty, and Security, MLAT requests submitted to the United States took an average of about ten months to be completed.[49] The delay in the processing of data requests, coupled with the denial of the request in many cases, has become a sore point for law enforcement agencies in other jurisdictions.

At the same time, at least part of the delay and denial of data requests can be attributed to requests that are incomplete or poorly drafted.[50] In a bid to address some of these issues, India's Ministry of Home Affairs recently released a new set of guidelines on the data request process. The stated objective of the guidelines, which also deal with the issue of summons and judicial documents, was to streamline the MLAT process and make it compliant with international norms. The guidelines set out a step-by-step guide for making MLAT/LR requests.[51] They contain instructions on the form, content, and language of requests as well as the grounds that the investigating agency should consider before initiating the request. These grounds could include an assessment of the necessity, timelines, potential grounds of refusal, legal basis, need for confidentiality, and limitation period.[52] The guidelines also offer a template of the request format.[53]

The standard forms and checklists given under the new guidelines offer a significant improvement over the existing process. Yet it is also important to acknowledge that neither the MLAT nor the LR processes were originally designed to handle the massive volumes or types of requests that they now experience. To put this in perspective, India's first MLAT with Switzerland was signed in 1989, well before the introduction of internet services in the country. Expecting the same systems to cope with the current situation of more than 700 million internet subscribers, and the increasing reliance of criminal investigations on electronic evidence, may well be a tall order.

To the extent that countries are able to seek direct access to subscriber information from service providers, the limitation of scope (limited to noncontent data) and significant discretion given to service providers remain a cause of concern for the authorities. At present, each service provider specifies its own mechanism through which law enforcement requests must be made. For instance, entities like Google, Twitter, and Facebook maintain separate systems through which law enforcement agencies can submit and track requests, while China-based TikTok specifies an email address to which the requests must be sent.[54] Some of the requirements in the processes adopted by different companies are that a lawful request should come from an official (not personal) email address; be issued on an official government letterhead; and should clearly identify the law at issue, the account whose details are being requested, and its link with the investigation. In addition, emergency data request mechanisms are also available for situations where the information being sought is necessary to prevent an imminent threat to a person's life or safety.

Interviews with service providers and their affiliate entities also brought to light certain issues that they face in the handling of data access requests by law enforcement agencies.[55] They highlighted that service providers often receive requests that contain errors, are missing important details, or seek information that is not available with the Indian affiliates of global businesses. Further, the requests

may contain unclear language or may not specify the legal provision under which the request is made. It was also pointed out that requests are sometimes sent based on defunct laws, such as section 66A of the Information Technology Act, 2000, which has been invalidated by the Supreme Court's decision in *Shreya Singhal* v. *Union of India*. Receipt of requests that are not sent from government email accounts was another repeated concern. One of the respondents also brought up the issue of receiving multiple requests for the same piece of information from different departments, and even from different persons within the same department.[56] All of these insights suggest that besides thinking about the scope of powers available to law enforcement agencies, improvements in their internal processes and capacity-building initiatives would also be in order.

Recommended Approach

The Ministry of Home Affairs' latest guidelines on handling of MLAT requests is an example of a unilateral effort by India for strengthening its existing MLAT enforcement. The United States also has undertaken an MLAT reform process that reportedly helped reduce its caseload backlog by a third.[57] Any kind of broader MLAT reforms, however, would have to be undertaken as a bilateral or multilateral initiative. This may include the renegotiation of existing agreements or entering into new ones, which can take place only through consensus among the contracting parties.

Accordingly, India will need to work with other nations to improve the existing MLAT framework. Such improvements may include increasing the geographic spread of such agreements and pursuing measures to reduce delays and enhance protection of human rights. Some specific suggestions that have been made in this regard are as follows:[58]

1. Increased resources, infrastructure, training, and digitization of the MLAT process

2. Strengthened due process requirements, including defendants' ability to request evidence

3. Improved privacy standards by incorporating requirements of necessity, proportionality, and encrypted transmission of data

4. Better transparency regarding requests and responses

However, as the following sections indicate, the willingness of state parties to undertake systemic MLAT reforms might be overshadowed by the shift in focus toward direct data access arrangements.

While India formulates its strategic position on such arrangements, it can take several steps at the domestic level to improve existing data access provisions.

First, India needs to develop robust and transparent SOPs (standard operating procedures) or guidelines on the process through which law enforcement agencies can request data access from service providers. The proposed SOPs must be grounded in existing laws. As the subject of "criminal procedure" falls under the concurrent list of the Constitution of India, the Ministry of Home Affairs can issue the proposed guidelines and, if required, each state government may modify them as appropriate.[59] Per an affidavit submitted by the central government before the Supreme Court, the government already has SOPs on this issue although a copy of it is not available in the public domain.[60] However, the current SOPs do not specify the agencies that are authorized to call for information under it and have also been criticized for the lack of accountability and appropriate safeguards.[61] An improved set of SOPs would, therefore, be in order.

Similar to the guidelines for mutual legal assistance requests, the guidelines for direct requests to service providers should specify the applicable step-by-step process; authorized agencies and officers; and the format, expected content, and language of the requests. The following list presents specific suggestions regarding the form and content of data requests sent to service providers.
Any request should be initiated only from an official government email address of a designated official of an authorized law enforcement agency.

1. It should be signed and on the letterhead of the requesting authority.

2. It should cite the legal provision under which the request is being made.

3. It should specify the number and details of the first information report and a brief note on the link between the case and the requested information.

4. It should clearly identify the scope of the data request, including the relevant identifier of the target for which data access is being requested.

Second, the guidelines referred to above should be framed through an open and consultative process. Once adopted, they should be incorporated in the training programs for police personnel, judicial officers, and staff of law enforcement agencies. In addition to the training on Indian laws and procedures on data access, it may be useful to include basic training on the laws and standards of certain

other jurisdictions that may have a significant bearing on cross-border data requests. For instance, the United States' Stored Communications Act is one such legislation, which limits the ability of U.S. service providers to provide certain kinds of data. Knowledge of such provisions can help law enforcement bodies in India understand the limitations of current cross-border access arrangements and take them into account while framing their requests.

Third, it would be useful to have a streamlined mechanism to transmit, authenticate, and complete requests being sent from law enforcement agencies to service providers. At present, each service provider maintains an independent system for managing data requests, making it necessary for law enforcement agencies to navigate these different systems. A new law enforcement data request platform could identify the various service providers to whom data requests are being sent and facilitate back-end integration with different providers while maintaining a common front-end platform for the law enforcement agencies. A streamlined system of this sort should include features like access controls and follow industry standards of encryption and other mechanisms to ensure secure data transmission.

Section 91 of the CrPC provides that an order summoning the production of a document or any other thing can be issued by a court or the "officer in charge of a police station." The proposed system, therefore, should be able to confirm that any request sent through it is verified to be from an officer that satisfies this condition—a consideration that a service provider may not find it easy to confirm on its own. The logs of information requests and responses exchanged on this platform can form the basis for necessary government transparency on the number and nature of data requests. Facilitating such enhanced transparency about data access requests for law enforcement purposes should be an integral part of the system's design.

Finally, inter-state and intra-agency coordination on data information requests should be enabled to ensure an optimum utilization of time and resources. For instance, the government of Jharkhand has put in place an Online Investigation Cooperation Request Platform, through which any investigating officer in the country can request authorities in Jharkhand for cooperation regarding investigation of cyber crimes.[62] The scope of such initiatives can be expanded to include collaboration on data requests being sent to service providers, where such data may be required by more than one authorized agency in connection with the same investigation. All such requests would, however, have to adhere to strict authentication requirements and security safeguards, including those listed in the first and second recommendations. This is to ensure that the proposed coordination mechanism should not become the basis for unchecked data sharing among government agencies.

The Move Toward Direct Data Access Agreements

Given the limitations of the existing cross-border data access arrangements, several countries have started looking toward alternative bilateral or multilateral arrangements to facilitate data access. This section discusses the growing popularity of direct data access agreements that essentially enable authorities in one jurisdiction to directly call for information from service providers based in another jurisdiction. The United States' CLOUD (Clarifying Lawful Overseas Use of Data) Act, enacted in March 2018, is the most-cited example of a law that enables the creation of such a framework. The CLOUD Act allows the United States to enter into executive agreements that will aid accelerated data access from U.S.-based providers by foreign partners.[63] At the multilateral level, the parties to the Council of Europe's Cybercrime Convention, popularly referred to as the Budapest Convention, have been negotiating an additional protocol that will contain provisions on direct access to subscriber data.[64] In parallel, the European Commission is also working on the adoption of an intra-EU arrangement to this effect.

Overview of Existing and Proposed Arrangements

The CLOUD Act amends the U.S. federal law on disclosure of information for investigation purposes in two main respects. First, it asserts the ability of U.S. government agencies to access data controlled by their electronic communication service or remote computing service providers, irrespective of the location where it is stored.[65] Second, it authorizes the U.S. government to enter into executive agreements with other countries allowing for direct data sharing by service providers, subject to the other country's laws and procedures satisfying the requirements laid down under the CLOUD Act.[66] The United States and the United Kingdom entered into the first such arrangement in October 2019 (hereinafter referred to as the "U.S.-UK executive agreement"), and the United States is currently negotiating similar agreements with Australia and the EU.[67] Interestingly, the head of the European Data Protection Board, Andrea Jelinek, recently wrote a letter in which she raised doubts about the data protection safeguards in the U.S.-UK executive agreement.[68] She also said that the European Commission should, when making the United Kingdom's adequacy finding under the General Data Protection Regulation, take the U.S.-UK executive agreement into consideration.[69]

The requirements for entering into an executive agreement under the CLOUD Act can be classified into two categories. In the first set of requirements, the U.S. attorney general, in concurrence with the secretary of state, determines that the other country's overall legal and procedural framework

satisfies certain conditions. These conditions include robust and substantive protections for privacy and civil rights, adherence to the rule of law and international human rights obligations, a commitment to promote the global free flow of information, and assurance that the agreement will not be used to target U.S. persons. The second set of requirements pertains more directly to the laws and processes governing data requests. This information includes specifications about the purposes for which data can be requested, reasonable justifications for the request, and judicial review requirements. The CLOUD Act also requires the U.S. government to periodically review the other party's compliance with the agreement.[70]

In terms of multilateral agreements, the Budapest Convention (to which India is not a signatory) is the only international treaty that deals extensively with international cooperation on the collection of electronic evidence for criminal offenses.[71] The convention provides for mutual assistance requests among parties that do not have MLATs among themselves and creates supplementary cooperation mechanisms that apply where MLATs are already in place. It currently allows unilateral access to data (without the need for the other party's authorization) only in two specific situations: for publicly available data and in cases where a party seeks to access data stored in another location through a computer system located in its own territory. The latter can be done only with the "lawful and voluntary consent" of the person who has the lawful authority to disclose it.[72]

Recognizing the vast changes in the technology sector since the Budapest Convention was first opened up for signatures in 2001, the parties to the convention are now working on an additional protocol for facilitating transborder data access.[73] As per the draft text of the Second Additional Protocol published in late 2019, state parties would be able to directly call for the disclosure of "stored subscriber information" controlled by service providers in the territory of another party.[74] The draft text lays out the contents of such an order and the manner in which it is to be processed. It also proposes the expedited production of subscriber or traffic data and data processing in emergency situations where there is a risk to any person's life or safety.[75] But, requests of this kind must still be sent from one state party to the other, and not directly to the service provider.

In case of direct requests, the draft gives each party the discretion to decide whether it would be bound by this provision or to exclude certain types of access numbers from its scope. Countries that do adopt the provisions have the further option of protecting their sovereign interests by voluntarily adopting some additional conditions. These conditions may include requirements relating to judicial approval or other form of independent oversight over the request, or simultaneous notification to the party in case of any information request sent to a service provider in its territory.

Finally, the European Commission is also working on the adoption of an intra-EU mechanism for direct access.[76] This mechanism would allow judicial authorities in one member state to seek the production or preservation of e-evidence by service providers established or represented in another member state. Service providers are expected to respond to the request within ten days with a shorter, six-hour deadline for emergency cases. The proposed e-evidence regulation will be accompanied by an EU directive obliging service providers to designate a legal representative in the EU to enable receipt of, and compliance with, the information requests.[77]

The e-evidence proposal was referred to the Civil Liberties, Justice and Home Affairs Committee (LIBE Committee) of the European Parliament for member comments. In November 2019, committee rapporteur Birgit Sippe released a draft report with significant revisions to the proposal.[78] The revisions seek to strengthen the respect of fundamental rights and introduce clearer obligations for service providers. The draft is now pending approval of the LIBE Committee before it can move to the next stage of legislative approval by the European Parliament.[79]

Key Provisions and Concerns

The goal of each of the direct data access agreements is to minimize the role of the other country's designated authorities in the review and approval of information requests, thereby reducing delays in the present systems. However, the current proposals for direct data access differ based on the kinds of data and crimes covered, requirements of judicial approval, procedural safeguards, and the rights of individuals and service providers. The proposed shift toward direct access also gives rise to concerns on grounds such as privacy, transparency, accountability, and lack of sufficient oversight. These issues have led many stakeholders, including privacy and civil liberties groups, to oppose the creation of direct assess measures based on the concern that they effectively make service providers the final guardians of human rights.[80]

This section presents some of the main differences between the different instruments and the concerns that have been raised about them. Table 1 below contains a comparative overview of some of the key terms contained in the U.S.-UK executive agreement, the draft Second Additional Protocol to the Budapest Convention, and the draft e-evidence proposal. This assessment does not include the CLOUD Act because, unlike the other instruments, it is domestic legislation and not a bilateral or multilateral arrangement.

TABLE 1

Overview of key provisions in direct access agreements

Bilateral/Multilateral Instrument	U.S.-UK Executive Agreement	Budapest Convention (Draft Second Additional Protocol—Direct Disclosure of Information)	EU e-Evidence Regulation (Draft)
Types of data covered	Broadest scope. Includes content data, traffic or metadata, and subscriber information.	Subscriber data only, specifically excludes traffic and content data.	Content (only stored) and noncontent (subscriber, access, transactional) data. The instrument cannot be used for interception requests.
Grounds for making data request	Any serious offense punishable by a maximum term of at least three years in the country issuing the request.	Information needed for the issuing party's specific criminal investigations or proceedings. The information must be necessary and proportionate to the criminal investigation or proceeding.	Orders for subscriber data and access data can be issued for all criminal offenses. Orders for transactional and content data may be issued only for serious criminal offenses (that is, offenses punishable by a maximum term of at least three years).
Judicial approval and independent oversight	Data requests subject to review or oversight by a court, judge, magistrate, or other independent authority. Authorization may be issued either before or during enforcement of the order. Because the requests are made as per domestic laws, requests from the United Kingdom for data stored in the United States must meet the standard of "reasonable grounds to believe" and not the more stringent "probable cause" standard under U.S. law.[81]	Data requests are to be made by a competent authority, which could be a judicial, administrative, or law enforcement authority. Prior authorization/ supervision is up to the discretion of the receiving country.	Orders for transactional and content data must be subject to judicial authorization. Orders for subscriber and access data can also be authorized by a prosecutor.

Bilateral/Multilateral Instrument	U.S.-UK Executive Agreement	Budapest Convention (Draft Second Additional Protocol—Direct Disclosure of Information)	EU e-Evidence Regulation (Draft)
Receiving state's right to receive notice	No requirement.	Not mandatory. The receiving state may require simultaneous notification when receiving a request. It can decide if it requires a notice for every case, or only in identified circumstances.	No requirement. However, the state issuing the request must seek clarification from the receiving state before making a request for any data that might affect immunities and privileges or otherwise impact the fundamental interests of the latter.
Individual's right to receive notice	No requirement.	No requirement. However, orders may contain "special procedural instructions" that may include a request for nondisclosure of the order to the subscriber or third parties.	The state issuing a data request can ask the service provider to refrain from sharing the information with the concerned person to avoid obstruction of the criminal proceedings. This information must be disclosed after a delay that is regarded to be necessary and proportionate.
Rights of service providers	Can raise specific objections when it has a reasonable belief that the agreement may not have been properly invoked. If unresolved with the issuing state's designated authority, it may raise the objections with the receiving state's authority.	No right or power to act, unless specified by the receiving state. In such a case, it shall consult with the receiving state's authorities on certain grounds, which include affecting the receiving state's ongoing criminal investigations or proceedings, sovereignty, public order, and so on.	Can oppose the enforcement of an order on various procedural grounds, and if it is apparent that it violates the charter of fundamental rights of the EU, or is manifestly abusive.
Consequences of noncompliance	Not specified.	No clear mention of consequences. However, states can provide "an affirmative basis obliging service providers to respond to orders from authorities from another state in an efficient and effective manner."	Pecuniary fines, without prejudice to penalties under national laws.

Scope of the Agreements

The scope of the data access arrangements can be understood to mean the available grounds for making a request and the types of data being covered. Of the three agreements, the U.S.-UK executive agreement is the broadest in scope as it applies to content data, traffic or metadata, and subscriber information.[82] Further, it covers both stored data and live communications (data in transmission). In essence, it allows any kind of data to be shared directly provided that it relates to a serious offense that is punishable by a maximum term of at least three years in the country issuing the request.[83]

The European e-evidence proposal also covers both content and noncontent data, but the scope of the former is limited to stored data only and so it cannot be used to make interception requests.[84] The grounds for access vary based on the type of data being requested. It proposes that orders for subscriber or access data can be issued for all criminal offenses, whereas transactional and content data can only be made for serious criminal offenses.[85] According to a report commissioned by the European Parliament's LIBE Committee, a threshold of three years' imprisonment for a "serious offence" would cover most offenses, including comparatively petty ones such as theft, fraud, and assault.[86] Civil society organizations also have raised similar arguments with respect to the CLOUD Act.[87] These objections might have had a bearing on LIBE rapporteur's recommendation that the threshold for serious offenses under the e-evidence proposal should be increased to a sentence of at least five years.

In contrast to the other two agreements, the Second Additional Protocol to the Budapest Convention plans to cover only subscriber data. By doing so, it presents a relatively lesser degree of threat to privacy, as disclosure of subscriber data arguably poses a lower risk compared to content and traffic data.[88] These limitations also may make the proposal more palatable to multiple contracting state parties. Nonetheless, submissions on the draft text have called for greater clarity in the definition of subscriber information. In particular, some submissions request that the designated information not include log-on or dynamic IP addresses, as these can reveal sensitive details about an individual's interests, beliefs, and lifestyle.[89]

Next, the draft provision allows the data request to be made for the purposes of "specific criminal investigations or proceedings" in the country issuing the request. The use of the term "specific" is meant to clarify that this power cannot be used to request mass or bulk production of data.[90] However, the provision does not draw any distinction based on the seriousness or severity of different crimes. This lack of distinction could result in a disproportionate impact on privacy while also opening the gates for large volumes of requests being made to service providers.[91] That said, such

criticisms must be tempered by the fact that access under the Budapest Convention would be limited to subscriber data, which in many cases is already shared directly. However, a key difference is that the procedure for disclosure of subscriber information under the Budapest Convention would be backed by a multilateral agreement, whereas the existing mechanisms are voluntary in nature, with each service provider having its own formats for information requests.

A final point of criticism involves the absence of any dual criminality requirements in the three instruments. Such requirements would mean that a direct request would be possible only if the act in question were an offense under the laws of both the issuing and responding states. In the context of the U.S.-UK executive agreement, a coalition of civil society groups has noted that even though MLATs typically do not have such requirements, its inclusion becomes particularly important for direct access arrangements because many of the oversight safeguards offered by MLATs have been removed.[92] Similar submissions have been made for the draft Second Additional Protocol.

Judicial Approval and Independent Oversight

One of the most serious criticisms of the CLOUD Act has been that it results in diminished standards of enabling data access.[93] By allowing foreign governments to access data without mandatorily satisfying the requirement of judicial authorization and "probable cause" under U.S. laws, individuals in countries with a weaker set of protections will be exposed to greater privacy risks. This could also result in the incidental targeting of U.S. communications through wiretaps set up without adherence to U.S. legal standards.[94]

Drawing on the language of the CLOUD Act, the U.S.-UK executive agreement requires that any data request made by the foreign government must be subject to review or oversight by a court, judge, magistrate, or other independent authority. This authorization can be issued either before or during the enforcement of the order.[95] The use of the term "other independent authority" leaves the agreement open for such a request to be reviewed by a nonjudicial body.

The Budapest Convention's proposal follows similarly broad criteria by allowing each country to determine a "competent authority" to issue the information requests.[96] This could be a judicial, administrative, or law enforcement authority. However, the country receiving the request can decide whether requests sent to its service providers should have been made under the supervision of a judicial, prosecution, or other independent authority.[97] In this sense, the Budapest Convention is more in the nature of an enabling framework with some discretion for the state parties to choose their preferred implementation structure.

In case of the EU's draft e-evidence regulation, the sanctioning authority varies depending on the type of data requested. Transactional and content data are subject to judicial authorization, but subscriber and access data, which are considered to be relatively less intrusive, could also be requested by a prosecutor.[98] Recognizing the concerns about the independence of prosecutors in some jurisdictions, the LIBE Committee's rapporteur has now recommended that such requesters should be an "independent" prosecutor. The rapporteur's draft report also proposes a new provision that would allow a party whose service provider receives the request to also require the procedural involvement of a court in its jurisdiction.[99] The involvement of judicial authorities in both jurisdictions would provide the highest degree of checks, but might also create delays in the process.

Right to Receive Notice

One of the other contentious issues raised by the data access arrangements relates to the extent to which the executing state or the affected individual should have the right to receive notice of the request. Of the three instruments, the protocol to the Budapest Convention is the only one that creates scope for notice to be given to the other state party; however, it does not make it mandatory to do so. It provides that a state party can choose to demand that its authorities should receive simultaneous notification.[100]

The draft e-evidence regulation contains a requirement to seek a clarification from the other party only in case of a data request that might affect immunities and privileges or otherwise impact the fundamental interests of the other party.[101] Recognizing the limitations of such a selective approach, many states have indicated the need for a more meaningful notification mechanism.[102] Accordingly, the draft report prepared by the LIBE Committee's rapporteur proposes an automatic notification mechanism for the executing state.

As far as notice to the individual is concerned, the draft e-evidence proposal is the only document that offers some protections in this regard. The current draft of the regulation allows the country issuing a data request to ask the service provider to refrain from sharing this information with the concerned person to avoid obstructing any criminal proceedings.[103] This information, however, needs to be disclosed after a delay that is regarded to be necessary and proportionate. The suggestions made by the LIBE Committee's rapporteur seek to strengthen this provision, such as by introducing the requirement that any request for delayed disclosure must be based on a court order.

By contrast, the draft Second Additional Protocol to the Budapest Convention states only that the order may contain any "special procedural instructions."[104] As per the accompanying explanatory text, this may include a request for nondisclosure of the order to the subscriber or other third parties.

Nonetheless, stakeholders have argued that the protocol should require that notice be provided to the individual, and gag orders delaying such notice should be for a specific time period and based on a judicial finding.[105]

The U.S.-UK executive agreement also gives rise to similar concerns. The position, as stated by the U.S. Department of Justice, is that it has been left to domestic laws of the country issuing the request to determine whether or how notice is to be given to the affected person.[106] This is a problematic omission, since the right to receive notice is a prerequisite for the individual to seek appropriate remedies against any unjustified interference with their rights.

In sum, much like the difference in the scope of each of the instruments, the protections and safeguards provided under them also tend to vary significantly. To some extent, the available protections reflect the nature of the instrument and the process through which it is finalized. The discussions around the e-evidence proposal and the Budapest Convention, which are more cooperative and multilateral in character, have offered greater transparency and opportunities for participation by stakeholders. These considerations have informed the recommendations in the next section on how India should approach participation in any bilateral or multilateral arrangements on direct access to data.

Proposed Approach for India's Engagement on Direct Data Access

Countries have at least three cooperative routes to address their increasing demands for access to cross-border data for law enforcement purposes. The first is to pursue systematic renegotiation and reforms in the MLATs framework. The goal here would be to simultaneously enhance the efficiency of the existing processes and strengthen the available safeguards. Given that MLATs tend to require the ongoing participation of both states' authorities, this route will require each of the state parties to commit appropriate time and resources for this purpose.

Second, countries could come together to create a new multilateral framework to regulate transborder access to personal data. Joseph A. Cannataci, United Nations special rapporteur on the right to privacy, has made a key suggestion on this topic.[107] In February 2018, Cannataci released a working draft of a legal instrument on government-led surveillance and privacy. The document suggests that any data request from a law enforcement authority of a member state would have to flow through a new body called the International Data Access Authority. The governing body of this authority would have representation from all the member states. Further, the authority would have a data

access commission of judicial members to review the requests, a committee of human rights defenders to monitor each request, and an international tribunal to hear appeals on the commission's decisions. An arrangement of this sort, if adopted by a significant number of countries, would create a powerful institutional structure to facilitate fair access. However, to date, the global community has not actively considered such a move or even begun to assess the feasibility and acceptability of the suggestion. Given the different strategic interests, access capabilities, and substantive and procedural requirements of various countries, any such move is bound to be subject to complex and protracted negotiations.

Meanwhile, as discussed in the earlier sections, many countries have already begun to proceed down the path of the third option of pursuing direct data access arrangements. Given the more real and immediate nature of this solution, this section focuses on potential factors of India's proposed approach to direct data access arrangements. So far, none of the existing and proposed discussions on this subject are applicable to India. India is not a signatory to the Budapest Convention and hence remains out of the fold of the ongoing negotiations on the Second Additional Protocol. Similarly, the e-evidence proposal, being an intra-EU arrangement, is not applicable to India. However, if other countries were to adopt these instruments, the ramifications would have a bearing on future agreements of this sort, including ones that India may subsequently enter.

There is no official position on the reasons for India's nonparticipation in the Budapest Convention, but some of the reported explanations include its absence from the original negotiations, concerns about infringement of national sovereignty, and the insufficiency of the cooperation mechanisms.[108] Given India's increasing demands for electronic evidence and the need for international cooperation and capacity-building initiatives in this regard, the Indian government should reconsider its position on the Budapest Convention. Recently, the government announced that it is planning to review the IT Act, the country's primary legislation related to cyber crime.[109] This review would be a good opportunity to initiate discussions on the Budapest Convention and data access agreements more generally.

Some commentators have suggested that India should also act on pursuing a bilateral agreement with the United States, along the lines set out under the CLOUD Act.[110] However, as of now, neither country has taken concrete steps that would indicate an interest in this direction. This lack of movement may result from a number of factors, including the fact that some of India's laws and practices are incompatible with several of the conditions under the CLOUD Act. For instance, one of the stated conditions is that an order issued by the foreign government should be subject to review by a court, judge, magistrate, or other independent authority. However, as noted earlier, a large number of requests in India are currently made directly by police officers under section 91 of the CrPC,

which does not satisfy this condition. Similarly, the requirements for appropriate laws, procedures, and oversight mechanisms for data collection and processing also are not likely to be satisfied in view of the broad exemptions proposed to be carved out for law enforcement agencies under the PDP Bill, 2019. At the same time, India may find some of the provisions of the CLOUD Act, such as commitment to the global free flow of information, as infringing on its national sovereignty concerns.[111]

The above discussions indicate that the CLOUD Act requires a level of legal and procedural safeguards that are higher than those currently provided under Indian laws.[112] A positive reading of the situation would be that if India were to consider an arrangement along these lines, it would necessarily involve domestic legal reforms of the kind suggested earlier. The contrary view, however, could be that the wording of the CLOUD Act gives U.S. executive agencies substantial discretion in deciding whether the other contracting party is able to adequately satisfy the stated requirements. A more liberal interpretation could, therefore, end up resulting in a situation where persons in India are exposed to a higher degree of domestic surveillance (including content data) but without the indirect safeguards that currently apply under U.S. legal requirements.

Realistically speaking, India is likely to be in a position to pursue any international agreements on direct data access only once it has undertaken certain domestic legal reforms. These reforms would have to establish the necessary legal safeguards and create appropriate implementation mechanisms to operationalize those requirements. The adoption of the PDP Bill, proposed revisions to the IT Act, and the outcome of the constitutional challenges to the surveillance provisions will be some of the important pieces of this puzzle. Yet even as these processes are underway, India should start to formulate its strategic position on international agreements for direct access to data for law enforcement purposes.

Keeping in mind the goal of ensuring more efficient data access, while adhering to a privacy-enhancing framework, India's thinking on this front should be informed by the preparation of a model international agreement on this subject. Similar model agreements have been adopted in the past, as in the case of bilateral investment treaties.[113] By putting in place a model agreement on cross-border data access, India can signal its starting position for future negotiations on this issue. Without this indicator, it runs the risk of being cornered by the starting position proposed by potential counterparties or leaving such important decisions to the discretion of a handful of negotiators.

To prevent such a situation, the duty of preparing the first draft of the proposed model agreement should be entrusted to a government-convened task force. The task force should consist of a diverse range of stakeholders, including representatives from different government departments, the private sector, civil society organizations, and experts in international law. The recommendations made by

the task force should be put out for public comments, with efforts to also encourage participation by international organizations and experts. The government should then publicly present the final draft of the model agreement prepared through this process, signaling India's starting position on any future negotiations on data access agreements.

In line with the suggested improvements to the domestic legal framework, the following basic safeguards should be considered while formulating India's model agreement on direct data access.

1. The scope of direct access should be limited to data required in connection with the prevention, investigation, or prosecution of serious crimes, which should be defined by taking into account a significant threshold of punishment. For instance, the threshold could be set to be a cognizable offense with an imprisonment of at least five years.

2. The order may be issued only with the prior approval of a judicial or other independent authority. Drawing from the text suggested by the United Nations special rapporteur on the right to privacy, any such approving body should be completely independent from the agency seeking the data and the executive or legislative branches of the government. Further, it should be composed of one or more members with the security of tenure of, or equivalent to, that of a permanent judge.[114]

3. There should be a mandatory requirement of notice to the affected individual—which may be a deferred notice, if necessary—along with an accessible mechanism for seeking redress. Further, the agreement should provide for simultaneous notification of the data request to the other party with specified grounds on which an objection may be raised.

4. The agreement should clearly spell out the grounds on which a service provider that receives a data request may challenge or decline to comply with the request and the consequences for the same.

5. The agreement should incorporate appropriate standards of data protection, including data minimization requirements and restrictions on transfer and sharing, and create a secure, encrypted system for exchanging data between the parties and service providers.

These recommendations stress the need to ensure that direct access to data should be recognized as an extraordinary remedy that bypasses some of the safeguards available under the MLATs route. Consequently, such remedies should be available for a narrower set of cases—namely, only the more serious offenses—while being subjected to a stricter set of standards. At the same time, further

research should explore avenues to improve the procedural safeguards and substantive protections in the MLATs framework, which would continue to cover a broader set of situations in which access to cross-border data may be required.

Conclusion

The importance of data access for law enforcement purposes is well recognized, as is the fundamental right to privacy. This paper has evaluated the ways in which India's present mechanisms for lawful data access can be improved to achieve better efficiency in cross-border access while respecting privacy rights. It highlights several concerns with India's current laws and practices on data access as well as the inadequacies of the present MLATs and LR processes. The subsequent discussion looks at the apparent shift in the international mood toward direct access arrangements that allow authorities in one country to directly seek information from service providers based in the other jurisdiction. It then offers an overview of the key provisions of such arrangements, as well as the concerns posed by the elimination of some existing safeguards.

The solution-oriented approach makes suggestions at three different levels. The first level involves the need for legislative amendments to ensure that India's legal regime will be able to comply with the requirements of lawful purpose, legitimate aim, proportionality, and procedural safeguards, as laid down by the Supreme Court, while upholding the right to privacy. The second level is that of framing guidelines and technological solutions to introduce greater efficiency and accountability in the present systems for data access by domestic law enforcement agencies. Notably, it should be possible to carry out these reforms even while the broader changes to the law remain in progress. The third level is that of international agreements for enabling data access, with a proposed process and basic safeguards that should inform India's future strategy on this issue. India should set up a multistakeholder task force to formulate a model international agreement on direct data access. Given the complexity of issues and interests, this model agreement should be formulated through an open and consultative process. Initiatives and reforms on all these three fronts can, and ideally should, be pursued simultaneously with the overarching goal of improving cross-border data access in a manner that enhances the protection of privacy and other human rights.

About the Authors

Smriti Parsheera is a researcher at the National Institute of Public Finance and Policy, and a fellow at the CyberBRICS project. Her areas of interest include privacy and digital rights, regulatory governance, and competition policy.

Prateek Jha is a program coordinator and research assistant at the Technology and Society Program at Carnegie India. His research focuses on issues related to data access and central bank digital currencies.

Acknowledgments

The authors are extremely grateful to Rudra Chaudhuri, Anirudh Burman, Arjun Kang Joseph, Rishab Bailey, Tarunima Prabhakar, and Vrinda Bhandari for their help and inputs.

Notes

1 *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, Court of Justice of the European Union, Case C-311/18 (July 16, 2020), http://curia.europa.eu/juris/documents.jsf?num=C-311/18#. This decision invalidated the EU's Decision 2016/1250 on the adequacy of the EU-U.S. Privacy Shield arrangement on the grounds that the protections available for the access and use of data transferred from the EU to the United States by U.S. public authorities did not meet the standards specified under EU law.

2 "The Indian Telecom Services Performance Indicators, October–December, 2019," Telecom Regulatory Authority of India (TRAI), June 30, 2020, https://www.trai.gov.in/sites/default/files/PIR_30062020.pdf.

3 Although this discussion paper focuses on criminal law enforcement, data access arguments also have come up in the context of the discharge of regulatory functions. For instance, access to data for regulatory purposes was given as a justification for the Reserve Bank of India's directive on localization of payments data.

4 "Frequently Asked Questions: New EU Rules to Obtain Electronic Evidence," European Commission, April 17, 2018, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345.

5 "Facebook Transparency Report," Facebook, accessed September 30, 2020, https://transparency.facebook.com/government-data-requests/country/IN.

6 Google received 19,438 user information requests in 2019 as compared to 6,901 requests in 2016; see "Google Transparency Report," Google, accessed September 30, 2020, https://transparencyreport.google.com/user-data/overview?hl=en&user_data_produced=authority:IN;series:compliance&lu=user_data_produced. Similarly, Twitter received 474 such requests from January to June 2019 as compared to 307 requests in the whole of 2016; see "Twitter Transparency Report," Twitter, accessed September 30, 2020, https://transparency.twitter.com/en/information-requests.html#information-requests-jan-jun-2019.

7 According to TRAI, the total number of internet subscribers in India increased from 391.5 million in December 2016 to 718.7 million in December 2019. See "Yearly Performance Indicators of Indian Telecom Sector (Second Edition)," Telecom and Regulatory Authority of India, May 4, 2017 and "The Indian Telecom Services Performance Indicators, October–December, 2019."

8 The six conventions are the United Nations Convention Against Transnational Organized Crime, 2000; United Nations Convention Against Corruption, 2003; United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substance, 1988; the Hague Convention; SAARC (South Asian Association for Regional Cooperation) Convention; and the Commonwealth Scheme (Harare Scheme).

9 Madhulika Srikumar et al., "India-US Data Sharing for Law Enforcement: Blueprint for Reforms," Observer Research Foundation and Cross-Border Requests for Data Project, Georgia Tech Institute for Information Security & Privacy, January 17, 2019, 39, https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf; and Drew Mitnik, "What's Wrong with the System for Cross-Border Access to Data?," *Access Now* (blog), April 25, 2017, https://www.accessnow.org/whats-wrong-system-cross-border-access-data. The interview with Stakeholder E (January 20, 2020) also addressed such concerns.

10 Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, *Report of the Committee of Experts under the Chairmanship of Justice B N Srikrishna*, Committee Report (India: Ministry of Electronics & Information Technology, Government of India, July 27, 2018), 88, https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf.

11 India, Personal Data Protection Bill, 2019, P.L. 373, 2019, accessed March 21, 2020, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf, Section 33. The bill does not define critical personal data, leaving this definition to be established by the government.

12 India, (Draft) The Information Technology [Intermediary Guidelines (Amendment) Rules], 2018, Ministry of Electronics & Information Technology, Government of India, accessed February 15, 2020, https://meity.gov.in/comments-invited-draft-intermediary-rules, rule 3(5) and 3(7).

13 Rishab Bailey and Smriti Parsheera, "Data Localisation in India: Questioning the Means and Ends," NIPFP Working Paper No. 242, National Institute of Public Finance and Policy, September 2018, https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf; and Jonah Force Hill, "Problematic Alternatives: MLAT Reform for the Digital Age," *Harvard Law School National Security Journal*, January 28, 2015, https://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/.

14 *Justice K. S. Puttaswamy* v. *Union of India*, Supreme Court of India, Writ Petition (Civil) No. 494 of 2012, accessed April 13, 2020, https://indiankanoon.org/doc/91938676/.

15 *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, Court of Justice of the European Union, Case C-311/18 (July 16, 2020), http://curia.europa.eu/juris/documents.jsf?num=C-311/18#.

16 Primrose Riordan and Mercedes Ruehl, "US Tech Groups Resist Hong Kong's Customer Data Access Plan," *Financial Times*, July 15, 2020, https://www.ft.com/content/77702487-0cec-4d88-990e-ffbcc69bf9df.

17 Rishab Bailey, Vrinda Bhandari, Smriti Parsheera, and Faiza Rahman, "Use of Personal Data by Intelligence and Law Enforcement Agencies," National Institute of Public Finance and Policy, August 1, 2018, https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf; "The Right to Privacy in India," Centre for Internet & Society and Privacy International, October 2016, https://privacyinternational.org/sites/default/files/2018-04/India_UPR_Stakeholder%20Report_Right%20to%20Privacy.pdf; and "India's Surveillance State," SFLC.in, September 2014, https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf.

18 Bedavyasa Mohanty and Madhulika Srikumar, "Hitting Refresh: Making India-US Data Sharing Work," Observer Research Foundation, August 2017, https://www.orfonline.org/wp-content/uploads/2017/08/MLAT-Book.pdf; and Amber Sinha, Elonnai Hickok, Udbhav Tiwari, and Arindrajit Basu, "Cross Border Data-Sharing and India: A Study in Processes, Content and Capacity," Centre for Internet & Society, February 2016, https://cis-india.org/internet-governance/files/mlat-report.

19 Elonnai Hickok and Vipul Kharbanda, "An Analysis of the CLOUD Act and Implication for India," Centre for Internet and Society, August 22, 2018, https://cis-india.org/internet-governance/files/analysis-of-cloud-act-and-implications-for-india.

20 Section 4, Indian Telegraph Act, 1885 and Rule 419A, Indian Telegraph Rules, 1951 deal with the interception of telegraphic messages while section 69 of the Information Technology Act (IT Act), 2000 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 framed under it provide for the interception of any other information. In addition, various surveillance enabling provisions are also provided for in the license agreements between the government and telecom service operators.

21 Ibid. The Telegraph Rules require a situation of "public emergency" or "public safety" to exist in addition to the specified grounds of sovereignty and integrity of India, security of the state, friendly relations with foreign states, public order, or preventing incitement of an offense. The rules under the IT Act, by contrast, do not require the two qualifying circumstances listed above and also expand the available grounds to include "defence of India" and the "investigation of any offence."

22 The following petitions challenging this order are currently pending before the Supreme Court: Manohar Lal Sharma vs. Union of India and others, W.P. (Criminal) No. 1 of 2019; Amit Sahni vs. Union of India and others, W.P. (Civil) No. 2 of 2019; Mahua Moitra vs. Union of India and another, W.P. (Civil) No. 13 of 2019; Shreya Singhal vs. Union of India and others, W.P. (Civil) No. 34 of 2019; Internet Freedom Foundation vs. Union of India and others, W.P. (Civil) No. 44 of 2019; and People's Union of Civil Liberties vs. Union of India and others, W.P. (Civil) No. 61 of 2019.

23 The government may grant this exemption if deemed "necessary or expedient" on grounds like sovereignty and integrity of India, security of the state, friendly relations with foreign states, and public order. The exemption also extends to the prevention of incitement to commit a cognizable offense relating to any of the above grounds.

24 The procedures notified by the rules framed under the Telegraph Act and the IT Act provide for executive orders and subsequent review by an executive-led committee. See the Indian Telegraph Rules, 1951 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009.

25 *People's Union of Civil Liberties* v. *Union of India*, AIR 1997, SC 568.

26 "India's Surveillance State," SFLC.in, September 2014, https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf.

27 "The Right to Privacy in India"; and "Surveillance – Is There a Need for Judicial Oversight?," SFLC.in, September 25, 2013, https://sflc.in/surveillance-there-need-judicial-oversight.

28 Rishab Bailey, Vrinda Bhandari, Smriti Parsheera and Faiza Rahman, "Placing Surveillance Reforms in the Data Protection Debate," The LEAP Blog, August 6, 2018, https://blog.theleapjournal.org/2018/08/placing-surveillance-reforms-in-data.html.

29 Vipul Kharbanda, "Transparency in Surveillance," Centre for Internet & Society, January 23, 2016, https://cis-india.org/internet-governance/blog/transparency-in-surveillance.

30 Manjeet Sehgal, "Himachal Pradesh Police Registers first FIR in Phone Tapping Scandal," *India Today*, June 28, 2013, https://www.indiatoday.in/india/north/story/himachal-pradesh-police-registers-first-fir-in-phone-tapping-scandal-168300-2013-06-28

31 Press Trust of India, "Chargesheet Filed in Arun Jaitley Phone Tapping Case," *Hindustan Times*, April 17, 2013, https://www.hindustantimes.com/delhi/chargesheet-filed-in-arun-jaitley-phone-tapping-case/story-4zntO5OKbdTG0swguTIbhP.html.

32 Ravi Kiran Jain and V. Suresh, "Going Beyond Telephone Tapping to Electronic Communication Surveillance: What Are the Safeguards for Citizens?," People's Union for Civil Liberties, January 25, 2019, http://www.pucl.org/press-statements/going-beyond-telephone-tapping-electronic-communication-surveillance-what-are.

33 For a discussion on the tests as laid down in the six opinions delivered by the different judges in the *Puttaswamy* case, see Vrinda Bhandari, Amba Kak, Smriti Parsheera and Faiza Rahman, "An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict," The LEAP Blog, September 20, 2017, https://blog.theleapjournal.org/2017/09/an-analysis-of-puttaswamy-supreme.html.

34 See the International Principles on the Application of Human Rights to Communication Surveillance (also referred to as the Necessary and Proportionate Principles) Coalition, https://necessaryandproportionate.org/. The principles suggest that any communications surveillance by the state must conform with the requirements of legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, user notification, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation, and right to effective remedy.

35 Bailey, Bhandari, Parsheera, and Rahman, "Use of Personal Data by Intelligence and Law Enforcement Agencies." The Justice Srikrishna Committee's report on data protection also mentioned some of these suggestions.

36 A lower threshold of, say, three years, would mean that seemingly less serious offenses, such as theft, extortion, criminal breach of trust, and dishonestly receiving stolen property, would also fall under its ambit.

37 This is in addition to the provisions that are already supposed to remain, such the requirement of a specific, clear and lawful purpose (section 4) and necessary security safeguards (section 24). See Rishab Bailey, Vrinda Bhandari, Smriti Parsheera, and Faiza Rahman, "Comments on the Draft Personal Data Protection Bill, 2019," The LEAP Blog, April 3, 2020, https://blog.theleapjournal.org/2020/04/comments-on-draft-personal-data.html.

38 Section 12, PDP Bill.

39 18 United States Code (U.S.C.) § 2702 and 2703.

40 18 U.S.C. § 2703 (d) lays down the requirements for sharing of content information pursuant to a court order.

41 The U.S.-India MLAT provides for the mutual assistance to be rendered by the two countries to each other for the investigation, prosecution, and prevention of offenses and proceedings in criminal matters. It also provides that the courts of the state receiving the request have the power to issue any necessary orders to execute the request (Article 15(1)), http://www.cbi.gov.in/interpol/mlat/UnitedStatesofAmerica.pdf.

42 18 U.S.C. § 2702.

43 India, "The Code of Criminal Procedure, 1973," Act No. 2 of 1974, accessed March 30, 2020, https://indiankanoon.org/doc/445276/, Section 166A.

44 India has designated the Cyber Crime Investigation Cell of the Central Bureau of Investigation as the contact point for the purposes of this network.

45 "Guidelines on Mutual Legal Assistance in Criminal Matters," Ministry of Home Affairs (MHA), December 4, 2019, https://www.mha.gov.in/sites/default/files/ISII_ComprehensiveGuidelines_17122019.pdf.

46 "The G8 24/7 Network of Contact Points Protocol Statement," Organization of American States, n.d., https://www.oas.org/juridico/spanish/cyber/cyb19_protocol_en.pdf. Generally, these data are preserved for an initial period of 90 days from the receipt of a request. During this period, the investigation agencies, including state law enforcement agencies, should send a proposal to IS-II Division, MHA, for issue of LR (Letters Rogatory) or MLA (Mutual Legal Assistance) Request for obtaining the data from concerned service provider. If the investigation is ongoing, then after every 60 days the request for preservation of data shall be served to the country concerned.

47 Thomas Dougherty, "G7 24/7 Cybercrime Network," n.d., https://rm.coe.int/1680303ce2.

48 Srikumar et al., "India-US Data Sharing for Law Enforcement," 41.

49 *Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World*, White House Archives, December 12, 2013, 227, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

50 Sinha, Hickok, Tiwari, and Basu, "CrossBorder Data-Sharing and India," 31.

51 "Guidelines on Mutual Legal Assistance in Criminal Matters."

52 Ibid., 17, Figure 3.1.

53 Ibid., 20–24, Figure 3.5.

54 "Sworn Law Enforcement Access," Google, n.d., https://support.google.com/legal-investigations/contact/records; "Guidelines for Law Enforcement," Twitter, n.d., https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support#11; "Law Enforcement Online Requests," Facebook, n.d., https://www.facebook.com/records/login/; and "Law Enforcement Data Request Guidelines," TikTok, August 13, 2020, https://www.tiktok.com/legal/law-enforcement?lang=en. TikTok also maintains an online system through which emergency data requests can be made.

55 Some of the interviews were conducted with the Indian affiliates of international service providers where the Indian entity is not directly involved in providing services to users and therefore is not the entity that is responsible for making decisions on law enforcement requests.

56 Interview with Stakeholder C, October 31, 2019; interview with Stakeholder F, October 18, 2019; and interview with Stakeholder J, February 21, 2020.

57 The U.S. Department of Justice's budget request for financial year 2019 referred to the "MLAT Reform" program being undertaken by their Criminal Division's Office of International Affairs since 2015. It reports that the backlog of MLAT requests had reduced from an all-time high of 13,421 in 2016 to 9,038 in 2019. See "FY 2019 Budget Request," U.S. Department of Justice, https://www.justice.gov/file/1033596/download.

58 Sinha, Hickok, Tiwari, and Basu, "CrossBorder Data-Sharing and India"; and Mohanty and Srikumar, "Hitting Refresh."

59 Item 2, List III, in the Seventh Schedule of the Constitution of India contains the entry on "Criminal procedure, including all matters included in the Code of Criminal Procedure at the commencement of this Constitution." As per Article 246 of the Constitution, the Parliament of India as well as the state legislatures have the power to make laws with respect to any of the matters enumerated in this list.

60 "Centre defends snooping notification in the Supreme Court," The Leaflet, March 11, 2019, https://www.theleaflet.in/centre-defends-snooping-notification-in-the-supreme-court/#.

61 "New insight into the Secret Operating Procedures of State Governments for Surveillance," Internet Freedom Foundation, September 25, 2019, https://internetfreedom.in/rti-on-state-surveillance/. Right to information requests filed by the Internet Freedom Foundation revealed that several state governments were following the central government's SOPs and some had adopted similar SOPs of their own.

62 Ankit Gupta and Gaurav Gaur, "Compendium of Best Practices in Smart Policing," FICCI SMART Policing Awards 2018, http://ficci.in/spdocument/22984/FICCI-Compendium-of-Best-Practices-in-SMARt-Policing-2018.pdf.

63 "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper," US Department of Justice, April 2019, https://www.justice.gov/opa/press-release/file/1153446/download.

64 "Preparation of the 2nd Additional Protocol to the Budapest Convention: State of Play," Cybercrime Convention Committee, July 8, 2019, https://rm.coe.int/t-cy-2019-19-protocol-tor-extension-chair-note-v3/16809577ff.

65 18 U.S.C. § 2713.

66 As per 18 U.S.C. § 2523(2)(b), the attorney general is required to determine the satisfaction of the stated requirements with the concurrence of the secretary of state and submit a certification of the same to Congress.

67 For the U.S.-UK executive agreement, see "Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, USA No. 6 (2019)," October 3, 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2.019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_

to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf. (For the U.S. version of the text, see https://www.justice.gov/dag/page/file/1231381/download.) The United Kingdom's enabling framework for entering into such an arrangement comes from the Investigatory Powers Act 2016, the Regulation of Investigatory Powers Act 2000, and Judicial Orders, For Australia, see "Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton," US Department of Justice, October 7, 2019, https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us.

68 Sam Clark, "UK Adequacy Woes Deepen," Lexology, June 16, 2020, https://www.lexology.com/library/detail.aspx?g=d355d242-dbba-46f0-8604-5277f34eeec3.

69 Ibid.

70 18 U.S.C. § 2511(j).

71 The convention creates a framework for mutual assistance requests among parties that do not already have MLATs or other similar arrangements among themselves. It also creates supplementary provisions for cooperation that apply even when a MLAT might already be in place.

72 Article 32, Budapest Convention.

73 The First Additional Protocol to the Budapest Convention was on xenophobia and racism committed via computer systems.

74 Cybercrime Convention Committee, "Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime," Council of Europe, T-CY (2018)23, November 8, 2019, https://rm.coe.int/provisional-text-of-provisions-2nd-protocol/168098c93c. (For the terms of reference of the Cybercrime Convention Committee, see https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b.) As per Article 18(3) of the Convention, subscriber information means any information relating to subscribers, other than traffic or content data, through which it is possible to establish the details of the type of communication service used or the subscriber's identity, address, payment information, or the like.

75 Article 1(d) of the Budapest Convention defines traffic data as the data that indicates the communication's origin, destination, route, time, date, size, duration, or type of underlying service. For emergency situations, see Articles 6 and 4 of the draft Second Additional Protocol to the Budapest Convention, respectively.

76 "European Commission, Security Union: Commission Receives Mandate to Start Negotiating International Rules for Obtaining Electronic Evidence," Press release, June 6, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2891.

77 The European Commission proposed the draft of the regulation and the directive on April 17, 2018. "E-evidence – Cross-border Access to Electronic Evidence," European Commission, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

78 Birgit Sippel, "European Production and Preservation Orders for Electronic Evidence in Criminal Matters, 2017," European Parliament Legislative Train Schedule, October 20, 2019, https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-jd-cross-border-access-to-e-evidence-production-and-preservation-orders.

79 Theodore Christakis, "E-evidence in the EU Parliament: Basic Features of Birgit Sippel's Draft Report," European Law Blog, January 21, 2020, https://europeanlawblog.eu/2020/01/21/e-evidence-in-the-eu-parliament-basic-features-of-birgit-sippels-draft-report.

80 "Consultations with Civil Society, Data Protection Authorities and Industry on the 2nd Additional Protocol to the Budapest Convention on Cybercrime," Council of Europe, November 21–22, 2019,

https://www.coe.int/en/web/cybercrime/protocol-consultations. See, for instance, submissions from the European Association of European Internet Services Providers Associations; Internet Service Providers Austria; and civil society organizations (Electronic Frontier Foundation, European Digital Rights, IT-Pol Denmark, Electronic Privacy Information Center).

81 "Promoting Public Safety, Privacy, and the Rule of Law Around the World," 12; and "Groups Urge Congress to Oppose US-UK Cloud Act Agreement," Human Rights Watch, October 29, 2019, https://www.hrw.org/news/2019/10/29/groups-urge-congress-oppose-us-uk-cloud-act-agreement

82 Article 1(3) of the U.S.-UK executive agreement. The U.S. Department of Justice provides answers to frequently asked questions on the purpose and impact of the CLOUD Act at https://www.justice.gov/dag/page/file/1153466/download.

83 Article 1(5) and (14) of the U.S.-UK executive agreement.

84 Articles 2(7) to (10) provide the definitions for subscriber data, access data, transactional data, and content data.

85 Articles 5(3) and 5(4) of the draft e-evidence regulation.

86 Martin Böse, "An Assessment of the Commission's Proposals on Electronic Evidence," Policy Department for Citizens' Rights and Constitutional Affairs, September 2018, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf.

87 "Groups Urge Congress to Oppose US-UK Cloud Act Agreement."

88 Content data is generally accepted to mean stored information revealing the actual contents of a communication (e.g., texts, emails, voice, videos, images), whereas traffic data indicates the communication's origin, destination, route, time, date, size, duration, or type of underlying service (Article 1(d) of the Budapest Convention). See "Conditions for Obtaining Subscriber Information in Relation to Dynamic Versus Static IP Addresses: Overview of Relevant Court Decisions and Developments," Cybercrime Convention Committee, October 25, 2018, https://rm.coe.int/t-cy-2018-26-ip-addresses-v6/168099388f.

89 "Consultations with Civil Society, Data Protection Authorities and Industry on the 2nd Additional Protocol to the Budapest Convention on Cybercrime."

90 "Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime," Explanation to Article 5, 22.

91 Submission made by the Center for Democracy & Technology on the Second Additional Protocol to the Budapest Convention, "Initial Observations of the Center for Democracy & Technology on the Provisional Draft Text of the Second Additional Protocol to the Budapest Convention on Cybercrime," November 8, 2019, https://rm.coe.int/cdt-comments-2nd-additional-protocol/168098c93e.

92 "Coalition Statement on the US-UK Could Act Agreement," Electronic Privacy Information Centre, October 29, 2019, https://epic.org/privacy/intl/USUK-CLOUD-Act-Letter-20191028.pdf.

93 "Groups Urge Congress to Oppose US-UK Cloud Act Agreement"; Camille Fischer, "The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data," Electronic Frontier Foundation, February 8, 2018, https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data.

94 "Groups Urge Congress to Oppose US-UK Cloud Act Agreement."

95 Article 5(2) of the U.S.-UK executive agreement. Also see 18 U.S.C. § 2523(4)(D)(v) for the corresponding provision under US laws.

96 Article 5(1) of draft Second Additional Protocol to the Budapest Convention.

97 Article 5(2)(b) of draft Second Additional Protocol to the Budapest Convention.

98 Article 4 of the draft e-evidence regulation.

99 Birgit Sippel, "Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters," Committee on Civil Liberties, Justice and Home Affairs, European Parliament, October 24, 2019, https://www.europarl.europa.eu/doceo/document/LIBE-PR-642987_EN.pdf.
100 Article 5(5)(a), draft Second Additional Protocol to the Budapest Convention.
101 Article 5(7), draft e-evidence regulation.
102 As per the LIBE Committee's rapporteur's report, eight member states (Czech Republic, Greece, Finland, Germany, Hungary, Latvia, Netherlands, and Sweden) submitted a joint letter dated November 20, 2018, containing a suggestion to this effect.
103 Article 11(2), draft e-evidence regulation.
104 Article 5(4)(f), draft Second Additional Protocol to the Budapest Convention.
105 See, for instance, submissions made by Centre for Democracy and Technology; Facebook; and the European Association of European Internet Services Providers Associations (EuroISPA) on the 2nd Additional Protocol to the Budapest Convention, n.d., https://www.coe.int/en/web/cybercrime/protocol-consultations.
106 "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper," U.S. Department of Justice, April 2019, https://www.justice.gov/opa/press-release/file/1153446/download.
107 Joseph A. Cannataci, "Working Draft Legal Instrument on Government-led Surveillance and Privacy (Version 0.7)," United Nations Special Rapporteur on the Right to Privacy, February 28, 2018, https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf.
108 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.
109 Navadha Pandey, "Govt Plans New IT Act to Factor in Cyber Crime, Data Privacy, New Tech," Live Mint, February 26, 2020, https://www.livemint.com/industry/infotech/plan-to-revamp-it-act-ravi-shankar-prasad-11582716511721.html.
110 Srikumar et al., "India-US data sharing for law enforcement."
111 Although the 2019 PDP Bill has a significantly softened position on data localization compared to the previous version drafted by the Justice Srikrishna Committee, it still contains some restrictions on cross-border data flows. More generally, India has been reluctant to make commitments on free data flows, particularly in the e-commerce sector.
112 See Hickok and Kharbanda, "An Analysis of the CLOUD Act and Implications for India."
113 The first version of India's model bilateral investment treaty (BIT) was released in 2003. This was replaced by a new model BIT in 2015—the official release by the new version by the Ministry of Finance, Government of India, was in January 2016. The adoption of this final version was preceded by the release of the draft text of the model BIT for public comments, which included review by the Law Commission of India. See Prabhash Ranjan and Pushkar Anand, "The 2016 Model Indian Bilateral Investment Treaty: A Critical Deconstruction," *Northwestern Journal of International Law & Business* 38, no. 1 (2017), https://scholarlycommons.law.northwestern.edu/njilb/vol38/iss1/1.
114 Cannataci, "Working Draft Legal Instrument on Government-led Surveillance and Privacy."

Unit C-5 & 6 | Edenpark | Shaheed Jeet Singh Marg | New Delhi, India 110016 | P: +011 4008687

CarnegieIndia.org