OBSERVER RESEARCH FOUNDATION

IKIGAI LAW

India's Proposed Data Protection Law and an India-US Executive Agreement under the Cloud Act

Sreenidhi Srinivasan and Osho Chhel

Attribution: Sreenidhi Srinivasan and Osho Chhel, *India's Proposed Data Protection Law and an India-US Executive Agreement under the Cloud Act*, June 2022, Observer Research Foundation.

Observer Research Foundation
20 Rouse Avenue, Institutional Area
New Delhi 110002
India
contactus@orfonline.org
www.orfonline.org

The Observer Research Foundation (ORF) provides non-partisan, independent analyses and inputs on matters of security, strategy, economy, development, energy, and global governance to diverse decision-makers (governments, business communities, academia, and civil society). ORF's mandate is to conduct in-depth research, provide inclusive platforms, and invest in tomorrow's thought leaders today.

Ikigai Law is an award-winning law and policy firm, with a sharp focus on technology and innovation.

This report has been developed with support from the Cross-Border Data Forum.

Design: Rahil Miya Shaikh

Layout: Simijaison Designs

CONTENTS

Executive Summary

INDIA CONTINUES TO DELIBERATE on a comprehensive data protection law. A Parliament panel examining the proposed legislation submitted its report in December 2021, paving the way for the Indian government to finalise the law and table it before Parliament. The proposed law governs how personal data can be collected, used, and shared to safeguard individual privacy. It calls for, among others, the local storage of certain types of data. Through such localisation mandates, the Indian government seeks to address challenges faced by law enforcement agencies (LEAs) in accessing data, stored by US service providers, that could assist in criminal investigations.

Meanwhile, the United States (US) Clarifying Lawful Overseas Use of Data Act or CLOUD Act offers an alternative approach to the same challenge. Enacted in 2018, the CLOUD Act provides an avenue for foreign law enforcement agencies to access evidence directly from US service providers in case of investigation of "serious crimes", through an executive agreement drawn up by the two countries for the purpose. To enter such an agreement with the US, a foreign country must meet certain procedural and substantive requirements, including having protections against surveillance and safeguards against unbridled government access to data. It also requires the partner country to show a commitment to an open and interconnected Internet, and to free flows of data across borders.

The United Kingdom (UK) was the first country to have entered into a CLOUD Act agreement with the US, in 2019. The negotiations between the two countries offer insights into how the US government is likely to interpret a foreign country's relevant laws, as well as lessons on potential obstacles to such an executive agreement. For instance, while examining the UK's legal regime, the US government scrutinised the obligations of UK authorities to meet purpose limitation, data minimisation, and other privacy principles enshrined in the EU General Data Protection Regulation (which was still applicable to the UK at the time). The US also evaluated the UK's independent oversight mechanism over interception warrants, through the 'Investigatory Powers Commissioner' and 'Judicial Commissioners' appointed for oversight. While UK law does not require judicial authorisation of every law enforcement request, the US found its mechanism of oversight through Judicial Commissioners to be sufficient. At the same time, to be able to enter into the agreement, the UK government also passed the UK Crime (Overseas Production Orders) Act 2019 (COPOA) that enables certain UK LEAs to apply for a UK court order with extra-territorial effect, compelling the production of electronic data stored outside the UK.

When assessed against CLOUD Act standards, India's existing data access laws may meet the mark in certain respects, but require additional protections on some fronts. As India finalises its data protection law, this report offers four key lessons from the US-UK negotiations under the US's CLOUD Act, evaluates existing Indian data access and surveillance laws, and ponders the proposed data protection law.

First, the UK-US negotiations showed that an overhaul of the foreign country's laws may not always be required to enter into an executive agreement with the US. The UK, instead of amending its entire set of laws, enacted the COPOA to give effect to the US-UK agreement and make direct requests to US service providers. Through the new law, the UK proposed the requirement of prior judicial oversight, for the sub-set of LEA requests to be made directly to US service providers. Similarly, given the difference in the US's and UK's approaches to free speech, the agreement provides for a review mechanism that will add another layer of evaluation for cases involving free speech offences, before requests can be made for evidence.

> Assessed against CLOUD Act standards, India's data access laws may meet the mark in certain respects, but require additional protections on some fronts.

Second, in the substantive assessment of laws, the US government may adopt a more lenient approach. For instance, while the UK Investigatory Powers Act does not require prior judicial authorisation for issuing interception warrants, the US Attorney General found the UK to have sufficiently clear mandates for access and oversight, through the review mechanism offered by the Investigatory Powers Commission and the Judicial Commissioners. However, for the sub-set of requests made under the US-UK agreement, a prior court order was presumably necessary – which is reflected in COPOA.

Third, India's upcoming data protection law could introduce protections that will bolster the country's case that it has robust protections for privacy and clear mandates for government access and oversight. For instance, positioning the data protection regulator as an additional layer of oversight over LEA requests, and requiring LEAs to abide by certain minimum privacy norms (such as data minimisation, purpose and retention limitations). In its current form, though, the draft law may only make it more difficult to explore a future CLOUD Act agreement as the US could view the wide exemptions to government agencies as disproportionate.

Finally, existing and proposed requirements for local storage of data in India could pose obstacles to a CLOUD Act agreement. However, given that the proposed law largely requires 'mirroring' rather than a hardline view on exclusive local data storage, there may still be room for negotiation in this regard.

I.
Introduction

LAW ENFORCEMENT AGENCIES (LEAs) IN INDIA often face challenges in accessing information stored by US service providers, which could be used in criminal investigations.[1] This experience is not unique to India, as US laws bar service providers from directly sharing communications content with foreign law enforcement agencies.[2] To access such evidence, LEAs, whether of India or of other countries, must use the framework of a mutual legal assistance treaty (MLAT)— a process that is generally described as long-drawn and cumbersome.

To enable foreign LEAs to access evidence from US service providers, the US enacted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in 2018. Among others, this law allows qualifying foreign governments to enter into bilateral agreements that will grant them direct access to communications content held by US service providers. To be eligible for such an agreement, the foreign government must meet the requirements laid out under the CLOUD Act. (The requirements are discussed in Section II of this report.)

So far, India has not pursued a CLOUD Act agreement with the US government. One reason could be the notion that Indian laws may not be able to meet the requirements set out under the CLOUD Act. For instance, the Fourth Amendment guarantee in the US Constitution requires LEAs to obtain a 'probable cause' warrant before they can conduct 'searches' related to a criminal investigation. This means that each law enforcement request is vetted by a court. In contrast, Indian criminal laws do not require prior judicial approval for LEA requests. Any police officer conducting a criminal investigation can

seek the production of any document simply by issuing a written order.[3] When the CLOUD Act was enacted, early commentary by Indian analysts suggested that this US standard of prior judicial approval (along with other substantive and procedural requirements) could be a cause of tension[4] and require India to amend existing laws to be eligible for an executive agreement.

Instead of pursuing bilateral arrangements, the Indian government sought to address the challenge of LEA access to evidence through local storage proposals. In the government's view, if data were to be stored within India, LEAs will be able to get access to it easily. Critics argue, however, that data localisation can create technical inefficiencies,[5] risk creating walled Internets, affect trade,[6] and raise rather than minimise security risks.[7] These observers also note that local storage of data will not remove the 'bar' under US law that restricts service providers from sharing evidence with foreign LEAs.[8] They propose instead that India strengthen other channels of data-sharing.

In 2019, one of the authors of this paper co-authored a report that explored India-US data-sharing for law enforcement.[9] The report highlighted bilateral and multilateral mechanisms for data-sharing and suggested the potential building blocks of an India-US CLOUD Act executive agreement. At the time of writing the 2019 report, there was limited guidance on how the US government would assess foreign governments against the CLOUD Act requirements. Since then, the US has concluded an agreement with the UK government (in 2019), and an agreement with the Australian government was also signed in December 2021.[10] The negotiations and the US Attorney General's assessment of UK's and Australia's laws offer useful guidance on interpreting the CLOUD Act requirements. This report focuses on the US's evaluation of UK laws.

The rest of this report is structured as follows. Following this Introduction, Section II describes the requirements of CLOUD Act. Section III then describes how UK laws fared in the US government's assessment on certain key parameters of the CLOUD Act. Section IV outlines the key surveillance laws in India, and tests them against the CLOUD Act standards. The fifth section discusses the Personal Data Protection Bill 2019 (PDP Bill) (now suggested to be renamed as the Data Protection Bill 2021), and ponders whether the law would make it easier for India to seek an executive agreement under the CLOUD Act. The report concludes with four key lessons for India when considering the possibility of an India-US CLOUD Act executive agreement.

While this report focuses on the CLOUD Act and how India fares on its requirements, similar conversations are taking place in other jurisdictions as well. Specifically, domestic surveillance laws are receiving increasing attention in discourses around international data transfers. In July 2020, the Court of Justice of the European Union (CJEU) invalidated the EU-US Privacy Shield since US law did not have enough protections for non-US citizens against surveillance. This has triggered the need to evaluate local surveillance laws for continued data transfers from the EU to other countries, including India[a]. Ironically, while the CJEU found US surveillance law to be inadequate, there are common themes between the CJEU's decision and the US CLOUD Act requirements, among them, oversight and clear rules for surveillance.

> "In the government's view, if data were to be stored within India, LEAs will be able to access it easily. Critics argue that data localisation can create technical inefficiencies and raise security risks."

a Implications of Schrems II on EU-India Data Transfers, August 21, 2022, https://community.nasscom.in/communities/policy-advocacy/nasscoms-study-implications-schrems-ii-eu-india-data-transfers.

II.

U.S. CLOUD Act: An Overview of Requirements

IN MARCH 2018, THE US passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act).[11] The law served two purposes. First, it clarified that the US government could order production of electronic evidence in the "possession, custody or control" of US service providers, regardless of where such evidence was stored.[12] Second, it allowed the US government to enter into executive agreements with foreign governments to allow foreign LEAs to access communications content directly from US service providers.[13] The US entered into the first such agreement in October 2019, with the UK government;[14] it signed an agreement with Australia in December 2021[15] and is in talks with the European Union (EU) as well.[16]

A. Overview

LEAs across the world often find it difficult to access evidence from US-based service providers.[17] LEAs argue that even for 'domestic' crimes, *i.e.*, where the perpetrator, victim, location of crime, are all in their local jurisdiction—the evidence remains inaccessible with a US service provider in the US or elsewhere.[18] These service providers are barred by US laws from sharing communications content,[19] and point the agency to the MLAT route. However, the MLAT process is cumbersome.[20] According to estimates, it takes an average of 10 months for a request to be completed.[21] The US CLOUD Act was passed to ease the process for foreign LEAs and allow them direct access to evidence held with service providers for certain serious crimes.

B. Entering into an Executive Agreement

The US government negotiates with its foreign counterpart to arrive at an agreement that meets the requirements laid down in the CLOUD Act. As part of this process, the US Attorney General, in concurrence with the US Secretary of State, must submit a written confirmation to the US Congress that the legal, procedural and substantive requirements in the Act have been met in the agreement.[22] This confirmation must be sent within seven days of the Attorney General certifying the agreement.[23] The US Congress then has 180 days to raise objections to the agreement, where congressional committees may seek further information on the details. Unless the Congress passes a joint resolution[24] within 180 days to reject the proposed agreement, it comes into force.[25] Thus, each new agreement must undergo scrutiny of the legal and foreign affairs branches of the US executive wing, as well as face any opposition in Congress.[26]

C. Procedural and Substantive Requirements in the US CLOUD Act

The CLOUD Act places guardrails on the kind of data access orders that may be issued and the procedural safeguards to be met for such orders. For one, orders must only be passed to seek data related to a "serious crime" such as terrorism.[27] Orders should be specific – concerning a person, address, device, or similar identifier.[28] There must be a reasonable justification for issuing such orders, grounded in credible and articulable facts.[29] The orders should be subject to independent review or oversight.[30]

The CLOUD Act also sets out substantive requirements to be met by the foreign country's laws. For a country to qualify under the Act, it must afford "robust" substantive protections for privacy and civil liberties in the context of government handling of data.[31] The government must demonstrate respect for the rule of law,[32] principles of non-discrimination,[33] and a commitment to international human rights.[34] Specifically, the government must afford protection from unlawful interference with privacy,[35] rights to a fair trial,[36] freedom of speech and expression,[37] prohibition on arbitrary arrests and detention,[38] and prohibition on torture and cruelty.[39]

The following paragraphs discuss two specific requirements: to have clear mandates for government access and effective oversight, and the commitment

to free flow of information and a global Internet. They are key to India as it finalises its data protection law.

D. Clear Mandates and Procedures for Government Access and Effective Oversight

Under the CLOUD Act, the US government must evaluate if the partner country has "clear legal mandates and procedures" for those LEA agencies that are authorised to seek data under the agreement. It requires foreign agencies to have procedures for collection, retention, use, and sharing of data, along with effective oversight of these activities.[40] The statute, however, does not clarify the benchmarks against which this assessment should be carried out.

At the same time, when discussing the requirements for an order under the CLOUD Act, the law only requires that the order be subject to review or oversight by a court, judge, magistrate, or other independent authority—[41] indicating that judicial authorisation is not the only permissible means of achieving an independent review. The order also does not need to be based on probable cause; only on a "reasonable justification" based on articulable and credible facts, particularity, legality, and severity regarding the conduct of the investigation.[42]

Since US legal process requires judicial authorisation of LEA requests, initial commentary on the CLOUD Act suggested that foreign countries may need to conform to the requirements of US legal processes to be deemed eligible for an executive agreement. For example, the Fourth Amendment[43] to the US Constitution guarantees protection against arbitrary and unlawful intrusions into privacy, and requires a judge to issue a warrant based on probable cause. This should be based on a fair possibility that incriminating evidence will be found.[44] Case laws on the Fourth Amendment also provide that surveillance must be "narrowly circumscribed"[45] for a "specific purpose", targeting a specific person for a particular piece of evidence.[46] This mechanism, therefore, has judicial oversight built into it as only a judge can issue such a warrant for probable cause. This has been reaffirmed in many cases, including *Riley v. California (2014),* where the US Supreme Court, reviewing the case of a mobile phone being seized without warrant, held that the judge must assess the degree to which the action would intrude upon individual privacy, on the one hand, and the legitimate state interest, on the other.[47]

However, the US DOJ has clarified that the countries are not required to have the exact same requirements as US laws.[48] At the same time, the DOJ said that the foreign government must provide accountability and transparency in its processes, and that some countries may need to improve procedures to be eligible.[49]

E. Commitment to Global Free Flow of Information and an Open Internet

The CLOUD Act requires the foreign country to show a commitment to the promotion and protection of the "global free flow of information" and the "open, distributed, and interconnected nature of the Internet."[50] The US has been a strong proponent of keeping borders open for free flows of data.[51] Notably, the US government has opposed localisation proposals of other countries, including India.

In the next section, this report discusses how both these requirements were interpreted by the US government in its assessment of UK's laws. This can offer a frame of reference for other countries seeking an executive agreement with the US.

III.

Lessons from the US-UK Negotiations

THE US-UK EXECUTIVE AGREEMENT WAS the first instance where the US government tested a country's laws against the CLOUD Act requirements. It therefore offers insights on the process a foreign country can expect, and the solutions or compromises made during negotiations. For instance, one contentious issue that emerged during the negotiations related to free speech protections, as UK laws contain certain prohibitions that are protected under the First Amendment of the US Constitution.[52] UK laws consider it an offence to send messages that are "indecent or grossly offensive" or "cause annoyance, inconvenience or needless anxiety" to the recipient.[53] Therefore, to meet CLOUD Act requirements, in the executive agreement, the US government retained the right to review requests from the UK that raise concerns on freedom of speech on a case-to-case basis.[54]

This next section examines the US's assessment of the two requirements discussed above—namely, clear mandates and procedures for government oversight, and a commitment to a free and open Internet.

For this, the US Attorney General's explanation[55] in determining that the agreement fulfills the CLOUD Act requirements is a useful guide. The assessment weighed UK laws against the thresholds set by the CLOUD Act's substantive and procedural requirements. Moreover, the US relied on its Department of State's report on human rights practices in the United Kingdom to prepare an overall assessment of the condition of freedoms in the UK.[56] The US is likely to utilise similar internal assessments to determine whether a country fulfills the substantive requirements under the Act.

A. Review of Relevant UK Laws

In the US-UK negotiations, the US government examined the UK Investigatory Powers Act (IPA),[57] read with the UK Data Protection Act (UK DPA).[58] The IPA governs interception of communications, and access to stored communications and metadata. At the time of negotiations, the UK DPA, along with the EU General Data Protection Regulation (GDPR), governed data-processing by the private and public sector, including LEAs.[59] The UK DPA also implemented the EU Law Enforcement Directive.[60]

The UK Data Protection Act 2018

The UK DPA sets out principles that LEAs must meet in processing data of individuals. These include: purpose limitation; restrictions on how much data should be collected; mandatory erasure of data; adoption of technical and organisational measures to safeguard data; and principles of privacy by design and by default.[61] For instance, the DPA provides that when personal data is processed for the purpose of law enforcement, such purpose must be specific, explicit, and legitimate; the data should not be excessive in relation to the purpose; the data should not be kept longer than necessary for that purpose; and there should be appropriate time limits for review of the need for continued storage.

LEA data controllers must also formulate internal policies on how they process sensitive personal data, demonstrating their compliance with the principles mentioned above; they are also required to regularly update these policies.[62] The DPA requires controllers (including LEAs) to implement "comprehensive but proportionate" accountability and governance measures.[63] These include the requirement to appoint data protection officers, to maintain documentation on data-processing activities, and to conduct data protection impact assessments when the processing could pose a high risk to individuals.

Further, the UK Information Commissioner's Office (ICO) monitors compliance with the DPA and with the EU Law Enforcement Directive, conducts investigations, and advises the Parliament and other parts of the UK government. Under the DPA, individuals may approach the ICO to seek redress in case the LEAs violate any principles, or to enforce the rights of erasure or rectification enjoyed by them under the DPA.[64]

UK Investigatory Powers Act 2016

The IPA identifies the public authorities that can apply for an interception warrant[65] or seek access to communications data.[66] It sets the standard of necessity and proportionality that must be met by the Secretary of State in issuing an interception warrant.[67] The IPA envisages a "dual lock" system where an interception warrant issued by the Secretary of State must be reviewed and approved by a Judicial Commissioner appointed under this law.[68] Authorities must periodically review data held by them so that it can be deleted when it is no longer required.[69]

The IPA provides for oversight through the Investigatory Powers Commissioner (IPC) and the team of Judicial Commissioners at the IPC Office.[70] The IPC Office oversees the exercise of warrants. The Judicial Commissioners are appointed by the prime minister for three-year renewable terms, on the joint recommendation of an independent appointments group. They are removable only by a resolution passed by Parliament or by the prime minister on certain limited grounds.[71]

B. Assessment of UK laws: Clear mandates for government access and Effective oversight

In assessing the UK DPA against the requirement for "clear mandates", the US Attorney General (AG) noted that the law is largely derived from the EU GDPR and the Law Enforcement Directive,[72] that are "widely recognized as establishing strict data protection and privacy rules."[73] Specific obligations on LEAs to adhere to purpose limitation, data minimisation techniques, and privacy by design[74] appear to be factors that convinced the Attorney General about the adequacy of the UK's data protection regime in relation to the CLOUD Act requirements. Similarly, the "dual lock" system under the IPA appears to have helped meet the threshold.

The AG's Explanation acknowledges the UK ICO's role in ensuring compliance with the principles and preventing government excesses.[75] Further, while not discussed in the AG's explanation, the "independent" nature of the ICO may have been an important factor in ensuring that the oversight mechanisms envisaged under the CLOUD Act operate meaningfully. The ICO has a fixed seven-year term, must be appointed based on "fair and open competition", and their removal requires Parliamentary approval on extremely specific grounds.

These statutory guarantees ensure that the agency responsible for oversight on other government agencies can operate fairly and independently.[76]

The IPA and the DPA work alongside each other, as the DPA governs data collected by government agencies through these warrants issued for interception and metadata collection. The AG concluded that read together, the laws provided clear legal mandates and procedures for LEAs that are authorised to seek data under the agreement, including procedures to collect/ retain/ use/ share data, and effective oversight of these activities.[77]

While examining the UK IPA, the Explanation specifically points to the independent nature of the oversight bodies and the independent appointment process for them.[78] Moreover, eventually, the UK enacted the Crime (Overseas Production Orders) Act 2019 (COPOA)[79] – which provides the legal authority for a judge to issue an overseas production order to be able to make a direct request to a service provider, pursuant to the US-UK agreement (which will be discussed in Section D).

C. Assessment of UK laws: Commitment to global free flow of information and an open Internet

Two reasons were cited as to why the UK meets the requirement that it demonstrate commitment to an open Internet and the free flow of information.[80] First, there is no law in the UK that requires businesses to store or process certain kinds of data within the territory. And second, the UK has opposed the implementation of data localisation laws in other countries. These two reasons give an indication of the criteria that the US will apply in determining whether a country meets this requirement.[81]

D. Other steps taken by the UK

To be able to enter into an agreement with the US, the UK government also passed the COPOA that enables certain UK LEAs to apply for a UK court order with extra-territorial effect, compelling the production of electronic data stored outside the UK. This could be done when the UK had an agreement with the country in which the foreign service provider was based. The law was enacted when the US-UK executive agreement was being negotiated—[82] to allow LEAs in the UK to make requests directly to foreign service providers, for when the CLOUD Act negotiations culminate.

The judge granting the request needs to be satisfied that there is a serious crime being investigated, that the targeted person is likely to have the information needed, and also that such information will be valuable to the investigation.[83] In the Explanation, the AG briefly mentions the COPOA to explain that UK laws contain the necessary legal safeguards for facilitating LEA access to data located abroad.[84]

Unlike the UK IPA, under which the Secretary of State can issue interception warrants, the COPOA authorises only a judge to issue "overseas production orders"— and thus, is closer to the US standard of prior judicial authorisation. Presumably this was required to be able to move forward with the negotiations.[85] Unlike US law, though, the COPOA does not require "probable cause" to be established. It is sufficient to have reasonable grounds to believe that the data in question will be of substantial value to the investigation.[86]

The above assessment offers a guide on pondering how Indian law may fare, when judged against the CLOUD Act requirements.

IV.

How India's Laws Fare on the CLOUD Act Parameters

THIS SECTION OUTLINES AN ASSESSMENT of Indian laws that are relevant to the two CLOUD Act requirements of: (i) clear mandates and procedures for government access and effective oversight; and (ii) the commitment to a free and open Internet.

Like with the UK, India's domestic laws and commitments to international human rights treaties will likely be examined by the US. A host of Indian laws govern data access by the Indian government and LEAs, including sectoral laws such as those governing the telecommunications, finance, and health sectors.

This evaluation focuses on the most prominent laws that govern surveillance and access to electronic data, drawing on the UK's experiences. The key laws likely to be examined are the following:

- The Information Technology Act 2000 (IT Act) and rules.[87] The IT Act governs the interception, monitoring and decryption of data in electronic form. Federal and state governments have the power to seek interception, monitoring or decryption of any electronic data in the interests of the sovereignty and integrity of India, the security of the State, public order, or to prevent incitement to an offence relating to these specific grounds.[88] The procedures and safeguards for such interception are prescribed through rules (Interception Rules).[89] Access to 'traffic data'[90] is prescribed through a separate set of rules (Traffic Data Rules).[91] The two sets of rules have similar procedures.

- The Telegraph Act and rules.[92] These set out the procedure for phone-tapping. The Interception Rules borrow heavily from the rules passed under the Telegraph Act.

- The Criminal Procedure Code 1973 (CrPC).[93] This governs the process for criminal investigations, including access to any evidence. Police officers routinely issue orders to tech companies for such data under the CrPC, which is the general criminal procedural law, rather than under the IT Act.

A. Procedures for interception, monitoring, and decryption of information

The Interception Rules require interception orders to be issued by a "competent authority",[94] i.e., the highest-ranking bureaucrat in the Home Ministry of the federal or state government.[95] In unavoidable circumstances, a junior-ranked government officer may issue these orders.[96] In "emergencies", the head of an authorised security agency/second most senior officer may also issue such orders.[97] However, such orders must be approved by the competent authority within seven days from the start of the interception.

Each order must be reasoned,[98] should specify the officer to whom the information will be disclosed,[99] be valid for a limited time period (60 days renewable up to 180 days).[100] Authorities must also consider "alternative means" and resort to decryption, interception, or monitoring only when other means are not possible.[101]

The Interception Rules also provide for the setting up of a review committee that will periodically review whether orders passed by the LEAs comply with the law. The review committee must assess these orders at least every two months.[102] If the review committee finds that the orders do not meet the procedures and safeguards, it can set aside these orders and ask for all accessed material to be destroyed.[103] The review committee is comprised entirely of government officers, and does not have independent judicial officers.[104]

B. General criminal procedural law: Used for access to stored data

The CrPC is the general law governing criminal procedure in the country. Under Section 91 of the CrPC, a police officer in-charge of a police station can issue a

written order seeking the production of any "document" from "the person in whose possession" such document may be.[105] A court can order the same thing through a summons. Police officers routinely take this route to seek access to email content and other data held by tech companies.[106]

In addition, Section 93 of the CrPC gives a court the power to issue a search warrant if it "has reason to believe" that a person may not comply with the order issued under Section 91.[107] This section also allows the court to issue "general warrants" to allow police officers to seek information, when it is unknown in whose possession such information may be.[108]

There are no other procedural safeguards, such as minimisation of data collected, restrictions on access, and retention periods for storage.

C. Analysis of Indian laws: Clear mandates for government access and effective oversight

As discussed above, the US CLOUD Act requires that the US government evaluate if the partner country has "clear legal mandates and procedures" for those LEAs that are authorised to seek data under the agreement, and if there are mechanisms for effective oversight of processing done by them.

Criminal Procedure Code

In India, general criminal law is commonly invoked in issuing orders to companies to share data. Within this, while the statute enables both a court and a police officer to compel production of data, the legal provision is more commonly used by police officers, without securing a court order. There are no other safeguards, and therefore this process might fail to pass the CLOUD Act threshold of clear mandates for access.[109] Arguably, any order issued by a police officer can be challenged before a criminal court (under whose jurisdiction the police officer may operate). There is little precedent of such orders being challenged, and it is difficult to conclude that this route would meet the standard for independent oversight.

In theory, though, one option is to use the judicial option envisaged by the CrPC.[110] To meet the CLOUD Act standard, a police officer must approach a court for issuance of a summons. While this may help satisfy the test for independent oversight, an agreement would also need to have other built-

in safeguards, such as restrictions around use of the collected data, who can access or view such data, retention periods, and other organisational and technical safeguards. It is worth recalling that when assessing the law governing interception in the UK (described in Part III.B of this report), the AG's Explanation points to the existence of safeguards such as the provision of authorising only specific entities to collect data, the periodic deletion of data, and the legal standards to be met for this data to be sought.[111]

Oversight Mechanism under the IT Act

Unlike the CrPC framework, the IT Act procedure does build-in some of these safeguards. However, the oversight mechanism, i.e., the review committee, and its independence has been questioned by privacy advocates. In December 2018, the government authorised 10 security agencies to issue interception orders.[112] Analysts argued that this was an indicator that such orders were routinely passed, and raised questions as to the efficacy of the surveillance process. The Rules were challenged before India's Supreme Court, for not ensuring independent oversight of surveillance orders.[113] The petitioner, Internet Freedom Foundation—a prominent digital rights organisation in India—argued that oversight by a different branch of the government (outside the executive) was a minimum requirement, and that judicial oversight was necessary to pass constitutional muster, as the judiciary alone could decide whether the measure was proportionate, balancing the importance of government's objectives against individuals' rights.[114] The matter is yet to be heard by the Supreme Court. Such concerns may resonate with the US government in its assessment of the surveillance laws.

India's new intermediary rules

In addition to the CrPC and the IT Act process, in February 2021, India updated its rules for digital intermediaries.[115] Under the new rules, intermediaries must meet a host of due-diligence requirements to be eligible for safe harbour protections for third-party content hosted on their platform. One such requirement is the need to appoint a chief compliance officer who is resident in India, who could face personal liability for non-compliance.[116] This may be viewed as limiting protections available to individuals—since intermediaries will have limited ability to challenge or evaluate LEA requests for meeting legal processes, given the risk of criminal liability for its employees.[117]

D. Analysis of Indian laws: Commitment to global free flow of information and an open Internet

In contrast to the UK, India has local data storage obligations. India's financial sector regulator, the Reserve Bank of India (RBI), requires payments companies to store payments data locally.[118] Moreover, under the proposed data protection law, companies must store 'sensitive personal data' and 'critical personal data' in India.[119] Such restrictions will likely be viewed adversely in determining India's commitment to a free and open Internet. The RBI's mandate, in particular, is a 'hard' data localisation requirement, i.e. payments data must be stored exclusively in India, and must be deleted from foreign servers even if taken outside India for processing.[120] This is a direct impediment to free flow of information, arguably more so than "mirroring" obligations. Such obligations are contained, for example, in the proposed data protection law (discussed in detail in Part V of this report), which allow transfers of data across borders with some safeguards, while requiring a "mirrored" copy to be stored within borders for LEAs to be able to access it when required for investigations. This practice will thus be harder to justify when judged against the CLOUD Act requirement for commitment to free information flows across borders.

E. Other potential issues

There are other CLOUD Act requirements where India could miss the mark—for example, restrictions on free speech under Indian laws prohibit certain types of speech, through the sedition[121] and blasphemy[122] provisions under the Indian Penal Code, 1860. As with the UK negotiations, questions about free speech protections could emerge, when set against those provided by the US First Amendment.

These potential issues—and the notion that India will need to amend its laws to be eligible for an agreement—could be the reason why India has been reticent in exploring a CLOUD Act agreement with the US. The upcoming data protection law may incrementally address some contentious issues, though it could also add more obstacles.

V.

The Proposed Data Protection Law

INDIA'S PROPOSED DATA PROTECTION LAW is a standalone law that governs data-processing by both private and government entities. The Personal Data Protection Bill 2019 or PDP Bill,[123] was tabled in Parliament in December 2019 and referred to a joint committee of the Parliament (JPC) for examination. The committee held consultations for nearly two years, and submitted its recommendations on 16 December 2021.[124] The JPC recommends, among others, renaming the law to Data Protection Act, dropping the word "personal" from the title. (For this report, though, we refer to the PDP Bill tabled in Parliament, flagging the JPC's recommendations where relevant.)

The data protection law is not intended to be a surveillance law. It does not update the existing surveillance and data access laws contained in either the IT Act, Telegraph Act, and the CrPC. Privacy advocates have been calling for surveillance reform in India for the past ten years or so. Many argue that the bill is a missed opportunity in that it could have been used to address gaps in the country's surveillance infrastructure.[125] Indeed, other members of Parliament have drafted bills that propose prior independent oversight on LEA requests.[126] It is unlikely, though, that the government will use this law to implement any significant surveillance reform.

A. Incremental Protections

The PDP Bill does offer some incremental protections around LEA access to data. While the law provides a near-complete exemption to processing for

investigation purposes,[127] there are a handful of provisions that still apply to data-processing for investigations.

First, the law requires the entity to show that processing is carried out for a "specific, clear and lawful purpose."[128] Arguably, this is an additional layer of protection to existing investigations, as LEAs must show that the purpose of data processing is "lawful". In 2017, the Indian Supreme Court unambiguously recognised a fundamental right to privacy, holding that any government action interfering with privacy must meet the test of necessity and proportionality.[129] Therefore, the requirement to show that processing is "lawful" can be interpreted as the need to demonstrate necessity and proportionality. However, the JPC suggests removing this clause—doing so will eliminate the requirement of specific, lawful, and clear purpose. If adopted by the government in the final version, this incremental protection from the 2019 draft law will be lost.

Second, the provisions related to the data protection authority will apply to data-processing activities connected to LEA investigations.[130] The establishment of the DPA and adjudication of complaints to the DPA are contained in chapter IX of the Bill. Data fiduciaries that process data for investigation are not exempt from chapter IX. This means that provisions relating to complaints and the DPA continue to apply to LEA investigations. This could mean an additional channel of redress for individuals, i.e., presumably, an individual can approach the independent data protection authority if they believe their data has been processed "unlawfully" by an LEA. These provisions could help address any concerns related to "independent oversight".

While these are small steps forward, they may bolster India's case in showing protections and oversight that is over and above what is provided in the Interception Rules and other surveillance laws. As a point of reference, the role of the ICO envisaged under the UK DPA was taken into account by the US government in assessing whether UK law has oversight mechanisms. India's data protection regulator could play a similar role here.

B. Additional obstacles

One concern with the Indian data protection regulator, as envisaged in its current form, is that it may fail to meet the "independence" threshold

required for effective oversight. The regulator will be appointed entirely by the executive,[131] raising concerns as to its insulation from the government and independence from the ruling executive. The JPC recommends the inclusion of technical, legal, and academic experts—to make the process more "inclusive, robust and independent".[132]

The proposed law also allows wide exemptions for government.[133] The government can exempt any of its agencies from the application of the law in its entirety for purposes like security of State, and public order. Any government order exempting an agency must also specify the procedure and oversight mechanism to be followed by the agency. Such wide exemption powers have come under heavy criticism from privacy advocates,[134] who argue that such blanket exemptions run afoul of the constitutional guarantee of privacy and will fail to meet the proportionality test.[135] The JPC further recommends that any procedure specified must be just, fair, reasonable, and proportionate. Whether this will suffice remains to be seen.

Moreover, unlike the UK DPA that requires LEAs to abide by principles of data minimisation, organisational and technical measures, and access controls, among others, the Indian draft law exempts LEAs from all other principles. A previous version of the law, which was recommended by an expert committee, had recommended additional protections, including the requirement to adopt security safeguards.[136] However, the current draft dilutes those, and offers wider exemptions, and the JPC retains this approach.

C. Local storage mandates: A potential deal-breaker?

The proposed law contains local storage requirements and restrictions on cross-border data flows. These requirements depend on the nature of data involved:

i. For "critical personal data" (CPD): This is an undefined category of data that will be determined through government notifications.[137] It is expected to include data that is sensitive from a national security perspective. Such data must be stored and processed almost exclusively in India.[138] It can be taken out of India under very narrowly defined circumstances.

ii. For "sensitive personal data" (SPD): This is a list of 11 categories of data including financial and health data.[139] This does not appear to be a

"hard localisation" requirement. While a copy of SPD must be stored or "mirrored" in India, it can still be transferred outside India under three conditions. These are somewhat similar to the GDPR restrictions on cross-border data flows, though arguably more restrictive since each of the conditions require recourse to the DPA/ government in some form. SPD can be transferred outside India under any of the following conditions: (a) a contract or an intra-group scheme approved by the DPA (it is unclear if this is meant to a case-by-case approval, which would be restrictive, or a model clauses approach similar to the EU standard contractual clauses); (b) the transfer is to a country approved by the central government (similar to the GDPR's ground of adequacy); and (c) the transfer is approved by the DPA.[140]

iii. For personal data that is not critical or sensitive: Such data can be freely transferred outside India.

The JPC examining the data protection law suggested additional restrictions on transfers of SPD. It suggests that the DPA must consult the central government before approving cross-border transfers pursuant to contracts or intra-group schemes or transfers for special purposes,[141] and such transfers can be disallowed if they run counter to "public policy" or "State policy".[142] It also proposes restrictions on onward transfers as an additional factor when determining adequacy.[143]

The JPC also calls on the Indian government to develop a comprehensive data localisation policy, and recommends that the government take steps to ensure that a "mirror copy" of SPD and CPD already in the possession of foreign entities is brought to India.[144] However, it does not recommend changes to the text of the law to this effect.

The US has been a strong proponent of free flows of data. The CLOUD Act requirement of global flows of data and an open and interconnected Internet will require the foreign country to show a demonstrable commitment to free cross-border data flows. In the case of UK, the fact that it did not have local storage mandates and objected to localisation proposals of other countries were key in arriving at a favourable outcome.[145]

When measured against UK restrictions on cross-border data flows, the proposed law is more permissive in certain aspects (i.e. it allows free flow of

personal data that is not sensitive or critical) but restrictive in certain others (i.e. SPD will include a wide ambit of data, the conditions for transfer could prove more restrictive than under UK law, especially if the condition on allowing transfers through a contract or intra-group scheme approved by the DPA is interpreted as a case-by-case approval, and there are mirroring requirements.)

Further, as discussed in Part IV.D of this report, India already has local storage requirements. For instance, the financial sector regulator, the RBI, requires local storage of payments data. In 2021, the RBI had proceeded against card issuers like Mastercard, American Express, and Diners Club, for failing to meet local storage norms,[146] signaling strong intent to take violations seriously. It is also unclear if the government will pursue the JPC's recommendation of bringing back mirror copies of SPD and CPD. This, along with the proposals in the PDP Bill, are likely to elicit a negative response from the US government.

However, given that the proposals in the PDP Bill are not blanket bars or hard data localisation mandates—in some respects, they are similar to restrictions on cross-border data transfers imposed by the UK—there could still be scope for negotiation.

VI.

A Possible India-US Executive Agreement: Four Takeaways for India

INDIA IS YET TO EXPLORE a CLOUD Act agreement with the United States. Part of the reason may be that, to explore an agreement, many believe that India will need to re-evaluate and amend at least some of its existing laws. At the same time, local storage mandates have emerged as a more appealing alternative, though critics argue that such mandates will take away technical and operational efficiencies and result in a fragmented Internet. This report offers four crucial takeaways.

First, the UK-US negotiations show that an overhaul of the foreign country's laws may not always be required before entering into an executive agreement with the US. Instead of amending its entire schema of existing laws, the UK enacted COPOA to give effect to the US-UK agreement and make direct requests to US service providers. In this new law, the UK proposed the requirement for prior judicial oversight, for the sub-set of LEA requests to be made directly to US service providers. Similarly, given the difference in approaches to free speech between the US and the UK, the agreement provides for a review mechanism, such that for cases involving free speech offences in the UK, there is an additional layer of review before direct requests can be made for evidence.

Second, in the substantive assessment of laws, the US government could adopt a more lenient approach. For instance, while the UK IPA does not require prior judicial authorisation for issuing interception warrants, the US Attorney General found the UK to have sufficiently clear mandates for access and oversight, through the review mechanism offered through the IPC and

the Judicial Commissioners. However, for the sub-set of requests made under the US-UK agreement, a prior court order was presumably necessary – which is reflected in COPOA.

Third, India's data protection law could offer certain additional protections to bolster its case that the country has robust protections for privacy and clear mandates for government access and oversight. For instance, adding the data protection regulator as an additional layer of oversight on LEA requests, or requiring LEAs to abide by certain minimum privacy norms (such as data minimisation, purpose limitation, retention limitations). In its current form, though, the draft law may only make it harder to explore a future CLOUD Act agreement. The wide exemptions to government agencies may be seen as disproportionate.

Finally, existing and proposed local storage requirements in India are likely to pose obstacles to an executive agreement. However, given that the proposed law to a large extent requires "mirroring" rather than a hardline view on exclusive data storage, there may still be room for negotiation.

VII.

Conclusion

THE CONDUCT OF THE US-UK NEGOTIATIONS suggests that the US does not expect the exact same protections in a foreign country's laws as are present in its own. For instance, it does not expect foreign countries to require "probable cause" warrants for LEA access. However, India's current approach to local data storage could prove to be a deal-breaker.

At this point, there is no indication from the Indian government that it is keen to pursue an executive agreement under the CLOUD Act. At the same time, the proposed data protection law provides India with an opportunity to close any gaps in existing data access laws. For instance, the upcoming law could introduce safeguards on government processing and subject government data-processing to scrutiny from the Data Protection Authority. This would be relevant not only for a potential CLOUD Act agreement, but also to bolster India's case for continued data transfers from the EU post-Schrems II,[147] and for any bid for adequacy under the EU GDPR.

> "The proposed data protection law gives India the opportunity to close gaps in its data access laws."

Endnotes

1 See comments from government officials: Neha Alawadhi, "CBI & FBI join hands to reduce time required to fulfil requests on information and evidence", *Economic Times*, December 07, 2015, https://economictimes.indiatimes.com/news/politics-and-nation/cbi-fbi-join-hands-to-reduce-time-required-to-fulfil-requests-on-information-and-evidence/articleshow/50069794.cms.

2 The US Electronic Communications Privacy Act, 1986 § 2512.

3 The Indian Criminal Procedure Code 1973 § 91.

4 See for e.g., E. Hickok *et al*, "An Analysis of the CLOUD Act and Implications for India," *Centre for Internet and Society*, pg. 17-18, August 22, 2018, https://cis-india.org/internet-governance/files/analysis-of-cloud-act-and-implications-for-india.

5 Erik van der Marel, Hosuk Lee-Makiyama, Matthias Bauer, *The Costs of Data Localization: Friendly Fire on Economic Recovery*, European Centre for International Political Economy, Occasional Paper No. 3/2014, 2014, https://ecipe.org/publications/dataloc/

6 Anupam Chander and Uyen P. Le, "Breaking the Web: Data Localization vs. the Global Internet," *UC Davis Legal Studies Research Paper Series, Research Paper No. 378*, (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858.

7 See Kalika Likhi, *India's data localization efforts could do more harm than good*, Atlantic Council, 2019, https://www.atlanticcouncil.org/blogs/new-atlanticist/india-s-data-localization-efforts-could-do-more-harm-than-good/

8 Madhulika Srikumar, comment on "Data localization is no solution," Observer Research Foundation, comment posted on August 3, 2018, https://www.orfonline.org/research/42990-data-localisation-is-no-solution/.

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

10 The United States Department of Justice, https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime.

11 Clarifying Lawful Overseas Use of Data Act, 2018 - H.R. 1625, http://www.crossborderdataforum.org/wp-content/uploads/2018/07/Cloud-Act-final-text.pdf.

12 The CLOUD Act § 2713. This mooted a question that arose in the Microsoft Ireland case, where the Supreme Court of the United States was examining whether warrants issued

under US law will be effective in case data is stored in another country. *United States v. Microsoft Corp*, 584 US _ 2018. See Justin Hemmings, Sreenidhi et al, "Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the CLOUD Act," Journal of National Security Law and Policy, Forthcoming, (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3469808.

13 The CLOUD Act § 2523.

14 The 'Agreement between the Government of UK and the Government of USA on Access to Electronic Data for the Purpose of Countering Serious Crime', https://www.justice.gov/dag/cloud-act-agreement.

15 The United States Department of Justice, https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us..

16 European Commission, European Union, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_5890.

17 Jennifer Daskal, "Unpacking the CLOUD Act," *EUCRIM*, no. 4 (2018), https://eucrim.eu/media/issue/pdf/eucrim_issue_2018-04.pdf#page=34.

18 Jennifer Daskal, "Unpacking the COUD Act".

19 The Electronics Communication Privacy Act, 1986 § 2511.

20 Jennifer Daskal, "Unpacking the CLOUD Act,". For the details of the MLAT process, see Chapter IV of Srikumar et al, India-US Data sharing for Law Enforcement, 2019, pg. 39, "US Data Sharing for Law Enforcement, Blueprint for Reforms".

21 Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein and Peter Swire, *Liberty and Security in a Changing World*, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, 2013, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

22 The CLOUD Act § 2523(b).

23 The CLOUD Act § 2523(d)(1).

24 The CLOUD Act § 2523(d)(4)(B).

25 The CLOUD Act §2523(d)(2).

26 See P. Swire et al, "Frequently Asked Questions (FAQs) about the U.S. CLOUD Act," *Cross Border Data Forum*, (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3469829.

27 The CLOUD Act § 2523(b)(4)(D)(i).

28 The CLOUD Act §2523(b)(4)(D)(ii).

29 The CLOUD Act §2523(b)(4)(D)(iv).

30 The CLOUD Act § 2523(b)(4)(D)(v). See The Software Alliance, *The CLOUD Act: Myth v Fact*, BSA, https://www.bsa.org/files/policy-filings/31318mythvsfactcloudact.pdf.

31 The CLOUD Act § 2523(b)(1).

32 The CLOUD Act § 2523(b)(1)(B)(ii).

33 The CLOUD Act § 2523(b)(1)(B)(ii).

34 The CLOUD Act § 2523(b)(1)(B)(iii).

35 The CLOUD Act § 2523(b)(1)(B)(iii)(I).

36 The CLOUD Act § 2523(b)(1)(B)(iii)(II).

37 The CLOUD Act § 2523(b)(1)(B)(iii)(III).

38 The CLOUD Act §2523(b)(1)(B)(iii)(IV).

39 The CLOUD Act § 2523(b)(1)(B)(iii)(V).

40 The CLOUD Act §2523(b)(1)(B)(iv).

41 The CLOUD Act § 2523(b)(4)(D)(iv).

42 The CLOUD Act § 2523(b)(4)(D)(v).

43 U.S. Const. amend IV. Under the Fourth Amendment, individuals have the right to "be secure in their houses, papers, and effects, against unreasonable searches and seizures".

44 See *Illinois v. Gates*, 642 US 213.

45 *Osborn* v. *United States*, 385 U.S. 323 (1966).

46 Aguilar v. Texas U.S. 108, 112 n.3 (1964).

47 See *Riley* v. *California*, 57

48 Promoting Public Safety, Privacy and Rule of Law Around the World - 2018, United States Department of Justice, *Frequently Asked Questions on the CLOUD Act*, 12 https://www.justice.gov/dag/page/file/1153466/download.

49 Promoting Public Safety, Privacy and Rule of Law Around the World, United States Department of Justice, *Frequently Asked Questions on the CLOUD Act*, https://www.justice.gov/dag/page/file/1153466/download.

50 The CLOUD Act § 2523(b)(1)(B)(iv).

51 See Kritika Suneja, "US, Japan and Singapore propose free flow of data, oppose server localization," *Economic Times*, May 4, 2018, https://economictimes.indiatimes.com/news/economy/policy/us-japan-singapore-propose-free-flow-of-data-oppose-server-localisation/articleshow/64020980.cms?from=mdr; S. Shanthi, "US, Japan and Singapore Agree for Cross-Border Data Flow as India calls for Data Localization," *Inc 42*, October 11, 2019, https://inc42.com/buzz/us-japan-agree-for-cross-border-data-flow-as-india-calls-for-data-localisation/.

52 Peter Swire and Justin Hemmings, "Recommendations for the Potential US-UK Executive Agreement under the CLOUD Act," Lawfare, September 13, 2018, https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act.

53 The Malicious Communications Act, 1988 § 1. https://www.legislation.gov.uk/ukpga/1988/27/section/1; Other laws prohibit sharing of "grossly offensive" material (Communications Act, 2003), "glorification" of acts of terrorism (Terrorism Act, 2006), "stirring up" of racial hatred (Public Order Act), or the disclosure of official secrets (Official Secrets Act, 1989).

54 Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, 2019 art. 8(4)(b).

55 See U.S. Department of Jusitce, Office of Legislative Affaits, *Materials conveyed to the US Congress in Support of the US-UK Cloud Act Agreement*. Washington D.C., 2019, https://www.justice.gov/dag/page/file/1231381/download.

56 See U.S. Department of State, *2018 Country Reports on Human Rights: United Kingdom*, White House, 2018, https://www.state.gov/reports/2018-country-reports-on-human-rights-practices/united-kingdom/.

57 The UK Investigatory Powers Act 2016.

58 The UK Data Protection Act 2018.

59 At the time of the negotiations, the Brexit process had not concluded, and the EU-GDPR was the relevant data protection legislation. After the UK's withdrawal from the EU, the UK passed the UK - General Data Protection Regulation that operates alongside an amended version of the UK DPA. International Commissioner's Office, "The UK GDPR," https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/.

60 See Information Commissioner's Office, "FAQs on Law Enforcement Processing," https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/law-enforcement-processing/.

61 The UK Data Protection Act, 2018 § 35-40.

62 The UK Data Protection Act, 2018 § 42.

63 Page 11, Explanation.

64 The UK Data Protection Act, 2018 § 51.

65 The Investigatory Powers Act, 2016 § 19-25.

66 The Investigatory Powers Act, 2016 § 60, 62, 63 and 65.

67 The Investigatory Powers Act, 2016 § 19.

68 Page 8, Explanation.

69 The Investigatory Powers Act, 2016 § 53.

70 Page 8, Explanation.

71 Page 8, Explanation.

72 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Criminal Justice Directive).

73 Page 9, Explanation.

74 The UK Data Protection Act, 2018 § 35-40.

75 See Page 11, Explanation.

76 See The UK Data Protection Act, 2018 Schedule 12.

77 Page 11, Explanation.

78 Page 8, Explanation.

79 The UK Crime (Overseas Production Orders) Act 2019.

80 Page 13-14, Explanation.

81 In addition, the Attorney General also considered the UK Country report, which states that the UK government did not restrict or disrupt access to the internet or censor online content, and there were no blanket laws covering internet blocking.

82 Charles Thomson, Joanna Ludlam, Jonathan Peddie, Tristan Grimmer, Henry Garfield and Yindi Gesinde, comment on "UK Introduces Crime (Overseas Production Orders) Act 2019 – Extension of the SFO's Evidence Gathering Power," Global Compliance News, comment posted June 26, 2019, https://www.globalcompliancenews.com/2019/06/26/uk-introduces-crime-overseas-production-orders-act-2019-extension-sfo-evidence-gathering-powers-20190506/.

83 The Crimes (Overseas Production Orders) Act, 2019 § 4.

84 Page 9, Explanation.

85 See Tim Cochrane, comment on "The Impact of the CLOUD Act Regime on the UK's Death Penalty Assurances Policy," U.K. Constitutional Law Blog, comment posted June 1, 2020, https://ukconstitutionallaw.org/2020/06/01/tim-cochrane-the-impact-of-the-cloud-act-regime-on-the-uks-death-penalty-assurances-policy/#:~:text=The%20UK%20passed%20the%20Crime,co%2Doperation%20agreement%E2%80%9D.

86 The Crime (Overseas Production Orders) Act, 2019 § 4(2).

87 Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

88 The IT Act § 69(1).

89 The IT Act § 69 (2), and the Interception Rules.

90 As per the explanation in Section 69B, IT Act, "traffic data" means "any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data, size, duration or type of underlying service or any other information."

91 Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

92 The Telegraph rules, 1951 Rule 419A.

93 Criminal Procedure Code, 1973 § 91.

94 The Interception Rules, Rule 3.

95 The Interception Rules, Rule 2(d).

96 The Interception Rules, Rule 3 First Proviso.

97 The Interception Rules Rule 3 Second Proviso.

98 The Interception Rules, Rule 7.

99 The Interception Rules, Rule 10.

100 The Interception Rules, Rule 11.

101 The Interception Rules, Rule 8.

102 The Interception Rules, Rule 22.

103 The Interception Rules, Rule 22.

104 The Telegraph Rules, 1951, Rule 419A(16).

105 The CrPC § 91(1).

106 "Zafarul told to join probe over controversial post," *The Hindu*, 1June 16, 2020, https://www.thehindu.com/news/cities/Delhi/zafarul-told-to-join-probe-over-controversial-post/article31837365.ece.

"JNU Attack: Google Says Court Order Necessary For Police to Access Chat Details," *The Wire*, June 16 2021, https://thewire.in/tech/jnu-attack-delhi-police-google-chat-details.

107 The CrPC § 93(1)(a).

108 The CrPC § 93(1)(b).

109 Smriti Parsheera and Prateek Jha, comment on "Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?" Carnegie India, comment posted November 23, 2020, https://carnegieindia.org/2020/11/23/cross-border-data-access-for-law-enforcement-what-are-india-s-strategic-options-pub-83197.

110 See Justin Hemmings, Sreenidhi Srinivasan and Peter Swire, comment on "How Stricter Procedures In Existing Law May Provide A Useful Path For Cloud Act Executive Agreements," Cross Border Data Forum, comment posted November 16, 2018, https://www.crossborderdataforum.org/how-stricter-procedures-in-existing-law-may-provide-a-useful-path-for-cloud-act-executive-agreements/ (accessed _____) and Justin Hemmings and Sreenidhi Srinivasan, comment on "Foundations of a Potential Executive Agreement between India and the U.S.," *ORF Digital Debates*, 2018, https://www.orfonline.org/wp-content/uploads/2018/10/Digital-Debates-Journal_v13.pdf.

111 Page 8, Explanation.

112 Javed Anwer, "10 govt bodies can now monitor and seize any computer, but calm down India is not a surveillance state yet," *India Today*, December 21, 2018, https://www.indiatoday.in/technology/talking-points/story/10-govt-bodies-can-now-monitor-and-seize-any-computer-but-calm-down-india-is-not-a-surveillance-state-yet-1414420-2018-12-21.

113 *Internet Freedom Foundation v. Union of India*, W.P.(C) No. 44/2019, Supreme Court of India.

114 Internet Freedom Foundation v. Union of India, W.P(C) No. 44/2019, Supreme Court of India at 124 in the petition.

115 See the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

116 The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(1)(a).

117 See for instance, Palais des Nations, *Mandates of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful association and the Special Rapporteur on the right to privacy*, Reference OL/IND 2021, 2021, *https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26385*.

118 Reserve Bank of India (RBI), *Storage of Payment System Data*, 2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244.

119 The Personal Data Protection Bill 2019 cl. 33 and 34. See Part IV of the paper.

120 Reserve Bank of India, *Frequently Asked Questions on Storage of Payment System Data*, 2019, https://m.rbi.org.in/scripts/FAQView.aspx?Id=130.

121 The Indian Penal Code, 1860 § 124A.

122 The Indian Penal Code, 1860 § 295A.

123 The Personal Data Protection Bill 2019.

124 Lok Sabha, *Report of the Joint Parliament Committee examining the Personal Data Protection Bill, 2019*, 2021, http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

125 Rahul Sharma, comment on "Contemporising Data Protection Legislation," Observer Research Foundation, comment posted February 01, 2021, https://www.orfonline.org/expert-speak/contemporising-data-protection-legislation/.

126 The Data Privacy and Protection Bill, 2017 cl. 108 and Chapter V. (a private members' bill by Dr. Shashi Tharoor of the Congress).

127 The Personal Data Protection Bill, 2019 cl. 36.

128 The Personal Data Protection Bill, 2019 cl. 4. Under Clause 36 of the PDP Bill, Clause 4 is not excluded from application to data processing for law enforcement purposes.

129 *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.

130 Under Section 36 of the PDP Bill, Chapter IX (Data Protection Authority of India) is not excluded from application to data processing for law enforcement purposes.

131 The Personal Data Protection Bill, 2019 cl. 42.

132 Lok Sabha, *Report of the Joint Committee on the Personal Data Protection Bill, 2019*, 2021 http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

133 The PDP Bill cl. 35.

134 *See* Internet Freedom Foundation, *A public brief and analysis on the Personal Data Protection Bill, 2019*, 2020 https://saveourprivacy.in/media/all/Brief-PDP-Bill-25.12.2020.pdf; Submissions to the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, *Mozilla.org* https://blog.mozilla.org/netpolicy/files/2018/10/Mozilla-Submission_MEITY_PDP-Bill-2018.pdf.

135 Renjithj Mathew, comment on "Personal Data Protection Bill 2019 – Examined through the Prism of Fundamental Right to Privacy – A Critical Study," The SCC Online Blog, comment posted May 22, 2020, https://www.scconline.com/blog/post/2020/05/22/personal-data-protection-bill-2019-examined-through-the-prism-of-fundamental-right-to-privacy-a-critical-study/.

136 See the Draft Personal Data Protection Bill, 2018, cl. 42(2)(f).

137 The PDP Bill Explanation to cl. 33(2).

138 The PDP Bill cl. 33(2) and 34(2).

139 Clause 2(36), PDP Bill lists the 11 categories of sensitive personal data, i.e., such personal data that may reveal, be related to, or constitute – financial data, health data, official

identifiers, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation, or any other types of data categorized as sensitive personal data by the government.

140 The PDP Bill cl. 34(1).

141 Lok Sabha, *Report of the Joint Committee on the Personal Data Protection Bill, 2019*, Para 2.149.

142 Lok Sabha, *Report of the Joint Committee on the Personal Data Protection Bill, 2019*, Para 2.150.

143 Lok Sabha, *Report of the Joint Committee on the Personal Data Protection Bill, 2019*, Para 2.154.

144 Lok Sabha, *Report of the Joint Committee on the Personal Data Protection Bill, 2019*, Para 1.15.17.5.

145 See page 13, Explanation.

146 George Mathew, "Explained: Curbs on foreign card firms," *The Indian Express*, July 17, 2021, https://indianexpress.com/article/explained/foreign-card-payment-network-curb-on-new-customers-rbi-restrictions-7408619/.

147 See Garima Prakash, comment on "NASSCOM study on 'Implications of Schrems II on EU-India data transfers'," Community by NASSCOM insights, comment posted August 12, 2021, https://community.nasscom.in/communities/policy-advocacy/nasscoms-study-implications-schrems-ii-eu-india-data-transfers; Caitlin Fennessy, "The 'Schrems II; Decision, EU-US Data transfers in Question," IAPP, comment posted July 16 2020, https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

About the Authors

Sreenidhi Srinivasan is a Principal Associate and Lead - Data, and **Osho Chhel** is an Associate at Ikigai Law.

The authors thank Ashish Agarwal, DeBrae Kennedy-Mayo, and Peter Swire for their comments and suggestions on the report, and Shrinidhi Rao (Associate, Ikigai Law) and Aditya Vats (former intern) for their research assistance.

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
contactus@orfonline.org
www.orfonline.org

Delhi | Bengaluru
contact@ikigailaw.com
www.ikigailaw.com