# An Analysis of the CLOUD Act and Implications for India

By: Elonnai Hickok and Vipul Kharbanda

## Introduction

India houses the second largest population in the world at approximately 1.35 billion individuals. In such a diverse and dense context, law enforcement could be a challenging job. Networked technologies have changed the nature of crime and will continue to do so.[1] Access to data generated by digital technologies and on digital platforms is important in solving online and offline crimes. Yet, a significant amount of such data is stored predominantly under the control of companies in the United States. Thus, for Indian law enforcement to access metadata (location data or subscriber information), they can send a request directly to the company. However for access to content data, law enforcement must follow the MLAT process as a result of requirements under the Electronic Communications Privacy Act (ECPA). ECPA allows service providers to share metadata on request of foreign governments, but requires a judicially issued warrant based on a finding of 'probable cause' for a service provider to share content data.[2]

The challenges associated with accessing data across borders has been an area of concern for India for many years. From data localization requirements[3], legal decryption mandates[4], proposed back doors[5]- law enforcement and the government have consistently been trying to find efficient ways to access data across borders.

Towards finding solutions to the challenges in the MLAT process, Peter Swire and Deven

[1]Wall, D. S. (2017). Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing.

[2] Electronic Privacy Information Centre. Electronic Communications Privacy Act (ECPA). Retrieved from https://epic.org/privacy/ecpa/

[3]The Economic Times (2018, 30 March). RBI note on data localisation raises hackles in the US. Retreived from https://economictimes.indiatimes.com/news/economy/policy/rbi-note-on-data-localisation-raises-hackles-in-the-us/articleshow/63966786.cms. and The Economic Times (2010, 30 August). RIM gives in, Blackberry server to be located in India. Retrieved from https://economictimes.indiatimes.com/tech/hardware/rim-gives-in-blackberry-server-to-be-located-in-india/articleshow/6462225.cms

[4]Section 69 of the IT Act provides authorized agencies with the power to intercept, monitor, and decrypt communications

[5]Techdirt (2015,September 21). India's Government Looking At Mandating Backdoors In Encryption. Retrieved from https://www.techdirt.com/articles/20150921/07085332311/indias-government-looking-mandating-backdoors-encryption.shtml

Desai in the article “A Qualified SPOC Approach for India and Mutual Legal Assistance” have noted the importance of finding a solution to the hurdles in the India - US MLAT and have suggested that reforms for the MLAT process in India should not start with law enforcement, and have instead proposed the establishment of a Single Point of Contact designated to handle and process government to government requests with requests emerging from that office receiving special legal treatment.[6]

Frustrations with cross border sharing of data are not unique to India and the framework has been recognized by many stakeholders for being outdated, slow, and inefficient - giving rise to calls from governments, law enforcement, and companies for solutions.[7] As a note, some research has also highlighted that the identified issues with the MLAT system are broad and more evidence is needed to support each concern and inform policy response.[8]

Towards this, the US and EU have undertaken clear policy steps to address the tensions in the MLAT system by enabling direct access by governments to content data. On April 17 2018, the European Union published the E-Evidence Directive and a Regulation that allows for a law enforcement agency to obtain electronic evidence from service providers within 10 days of receiving a request or 6 hours for emergency requests and request the preservation or production of data. Production orders for content and transactional records can be issued only for certain serious crimes and must be issued by a judge. No judicial authorisation is required for production orders for subscriber information and access data, and it can be sought to investigate any criminal offense, not just serious offenses. Preservation orders can be issued without judicial authorisation for all four types of data and for the investigation of any crime.[9] Further, requests originating from the European Union must be handled by a designated legal representative.[10] Preservation orders can be issued for all four types of data.[11] Further, requests originating from the

---

[6]Swire P and Desai D., Lawfare (2017, March 02). A “Qualified SPOC” Approach for India and Mutual Legal Assistance. Retrieved from https://www.lawfareblog.com/qualified-spoc-approach-india-and-mutual-legal-assistance

[7]Non-paper from the Commission services.Improving cross-border access to electronic evidence:Findings from the expert process and suggested way forward.Retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

[8]Carrera S (2015). Access to Electronic Data by Third-Country Law Enforcement Authorities Challenges to EU Rule of Law and Fundamental Rights.https://www.ceps.eu/system/files/Access%20to%20Electronic%20Data%20%2B%20covers_0.pdf

[9]https://www.insideprivacy.com/uncategorized/eu-releases-e-evidence-proposal-for-cross-border-data-access/

[10]https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

[11]Covnigton (2018, May 08). "EU Releases e-Evidence Proposal for Cross-Border Data Access", Retrieved from https://www.insideprivacy.com/uncategorized/eu-releases-e-evidence-proposal-for-cross-border-data-access/

European Union must be handled by a designated legal representative.[12]

On the US side, in 2016, the Department of Justice (DoJ) put out draft legislation that would create a framework allowing the US to enter into executive agreements with countries that have been evaluated as meeting criteria defined in the law.[13] Our response to the DoJ draft Bill can be found here.[14] In February 2018, the Microsoft Ireland Case was presented before the U.S Supreme Court. The question central to the case was whether or not a US warrant issued against a company incorporated in the US was valid if the data was stored in servers outside of the US. On March 23, 2018, the United States government enacted the "Clarifying Lawful Overseas Use of Data Act" also known as the CLOUD Act. The passing of the Act solves the dilemma found in the Microsoft Ireland case.[15] The CLOUD Act amends Title 18 of the United States Code and allows U.S. law enforcement agencies to access data stored abroad by increasing the reach of the U.S. Stored Communication Act[16], enabling access without requiring the specific cooperation of foreign governments. Under this law, U.S. law enforcement agencies can seek or issue orders that compel companies to provide data regardless of where the data is located as long as the data is under their "possession, custody or control". It further allows US communication service providers to intercept or provide the content of communications in response to orders from foreign governments if the foreign government has entered into an executive agreement with the US upon approval by the Attorney General and concurrence with the Secretary of State. The Act also absolves companies from criminal and civil liability when disclosing information in good faith pursuant to an executive agreement between the US and a foreign country. Such access would be reciprocal, with the US government having similar access rights to data stored in the foreign country.

Though the E-Evidence Directive is a significant development, in this article - we focus on the CLOUD Act and its implications for cross border sharing of data between India and the US.

---

[12]European Commission.E-evidence - cross-border access to electronic evidence. Retrieved from https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

[13]Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purpose of Combating Serious Crime Including Terrorism. Retrieved from https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p4

[14]Hickok E and Kharbanda V,.Cross Border Cooperation on Criminal Matters - A Perspective from India. Retrieved from https://cis-india.org/internet-governance/blog/cross-border-cooperation-on-criminal-matters

[15]Daskal J., (2018, May), Microsoft Ireland, the CLOUD Act, and International Lawmaking 2. Retrieved from https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/

[16]18 U.S. Code § 2513 - Confiscation of wire, oral, or electronic communication intercepting devices.

**India and the CLOUD Act**

If there is a need for the Indian government and the US government to pursue an Executive Agreement as envisaged under the CLOUD Act, the Agreement will have to be certified by the Attorney General of the United States as satisfying the requirements of Section 2523 of the United States Code. The consensus amongst academic scholars appears to be that the phrase "factors to be met" implies that each of the factors articulated in the Act have to be satisfied for Indian laws to qualify for an Executive Agreement.[17]

This certification has two parts; (i) a determination as to the adequacy of *Indian law and its implementation* in regard to substantial and procedural safeguards for privacy and civil liberties as defined in the Act; and (ii) a determination that the provisions of the Agreement satisfy certain conditions and requirements as defined in the Act. Such determination must take into consideration appropriate, credible and expert input.

In order to make the first determination on adequate substantive and procedural laws privacy and civil liberties,[18] the Attorney General is required to assess India's legal framework against the different criteria discussed below:

1. **Substantive and Procedural Laws on Cybercrime and electronic evidence:** *This includes the presence of laws on cybercrime and electronic evidence. This can be demonstrated in two ways: (i) through being a party to the Budapest Convention on Cybercrime, or (ii) by having laws consistent with chapters I and II of the Convention.*

**Law and Policy:** At the outset it must be said that while there are a number of non-European Union States that are signatories to the Budapest Convention on Cybercrime, India is not one of them. However, this section allows for the domestic laws of the country to be consistent with the definitions and requirements set forth in the Convention. The primary legislation dealing with cybercrime in India, the Information Technology Act, 2000 (ITA) has penal provisions which heavily reflect the provisions of the Budapest Convention. However, further analysis may be needed to find whether the domestic laws of India are consistent with the definitions and requirements set forth in Chapters I and II of the Budapest Convention. Though India has not signed the Convention and has traditionally pushed back against the same for a variety of reasons[19], in 2018, there has

[17] Peter Swire, Jennifer Daskal. What the CLOUD Act means for privacy. iapp. Available at: https://iapp.org/news/a/what-the-cloud-act-means-for-privacy-pros/

[18] Although a strict reading of the CLOUD Act provides that the Attorney General has to give a separate certification on data minimization practices, however in the interest of brevity, that determination has been clubbed with the discussion on the more generic determination about the substantive provisions of Indian law.

[19] Seger A., India and the Budapest Convention: why not?. Retrieved from https://rm.coe.int/16806a6698

been indication from some parts of the government that this position may be reconsidered.[20] It will be interesting to see if the CLOUD Act influences this decision to any extent.

With respect to the rules for electronic evidence, one of the primary objectives of the ITA was to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, and to facilitate electronic filing of documents with the Government agencies.[21] Further sections 65A and 65B of the Indian Evidence Act, 1872 provide a detailed procedure for proving the contents of an electronic record.

In 2017, the Supreme Court of India recognized privacy as a fundamental right, but India lacks a comprehensive privacy legislation, despite multiple moves towards this.[22] India's surveillance regime for lawful access to data is spread across three laws and license agreements - section 69 and 69B and associated Rules of the ITA which enables authorized agencies to intercept, decrypt, and monitor communications and traffic data; section 5 and the 419A Rules of the Indian Telegraph Act, 1885 (TA) allows for interception of communications; section 91 of the Cr.P.C. allows for access to stored data including content data. The Unified Access Service License under the Telegraph Act places a number of security requirements on service providers including requirements for surveillance capabilities.

**2. Rule of Law and Non-discrimination**: *Indian law and practice must show evidence of respecting the rule of law and principles of non-discrimination*.

**Law and Policy:** India has adopted the common law system which originated in English jurisprudence, the basis of which is the Rule of Law. The theory of Rule of Law states that the state is governed by a set of written laws which are supreme and govern all people equally. It is widely accepted that India is a country governed by the rule of law and the biggest evidence of this fact is the supremacy of the Constitution of India as the supreme law governing all people irrespective of their standing. The specific inclusion of the

[20]Indian Express (2018, January 18) Home Ministry pitches for Budapest Convention on cyber security. Retrieved from https://indianexpress.com/article/india/home-ministry-pitches-for-budapest-convention-on-cyber-security-rajnath-singh-5029314/

[21] Section 4 of the Act provides that where any law requires that any matter needs to be in written form then that requirement shall be deemed to be satisfied if the matter is available in electronic form.

[22]For example: In 2012, Justice AP Shah chaired a group of experts that published recommendations towards a privacy framework in India. The Report of Group of Experts on Privacy is available at: http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf
In 2017 SriKrishna chaired a committee that undertook a similar exercise and produced a white paper towards a privacy framework for India. The SriKrishna White Paper on Data Protection is available at: http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf

principle of equality under Article 14 further demonstrates that the legal regime in India is committed to the rule of law and the principles of non discrimination. India also has in place the Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act, 1989, which was amended in 2015 to expand the scope of offences of caste discrimination.

**Practice:** India may be required to demonstrably strengthen its practices around non-discrimination and commitment to the rule of law. Though anti-discrimination laws are in place, reports have cited crime statistics on offences relating to caste based discrimination.[23]

**3. International Human Rights**: *Adherence to international human rights obligations including protection from arbitrary and unlawful interference along with privacy, fair trial rights, freedom of expression, association, and peaceful assembly, prohibitions on arbitrary arrest and detention, prohibitions against torture and cruel, inhuman, or degrading treatment or punishment.*

**Law and Policy:** As noted in our earlier blog - "*India is a signatory to a number of international human rights conventions and treaties, it has acceded to the International Covenant on Civil and Political Rights (ICCPR), 1966, International Covenant on Economic, Social and Cultural Rights (ICESCR), 1966, ratified the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), 1965, with certain reservations, signed the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), 1979 with certain reservations, Convention on the Rights of the Child (CRC), 1989 and signed the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT), 1984. Further the right to life guaranteed under Article 21 of the Constitution takes within its fold a number of human rights such as the right to privacy. Freedom of expression, right to fair trial, freedom of assembly, right against arbitrary arrest and detention are all fundamental rights guaranteed under the Constitution of India."*[24] In addition, India has enacted the Protection of Human Rights Act, 1993 for the constitution of a National Human Rights Commission, State Human Rights Commission in States and Human Rights Courts for better protection of "human rights" and for matters connected therewith or incidental thereto. Thus, there does exist a statutory mechanism for the enforcement of human rights[25] under Indian law. It must be noted that the definition of human rights also incorporates rights embodied in

[23]Deshpande A., (2017, December 11). The Ugly Reality of Caste Violence and Discrimination in Urban India. Retrieved from https://thewire.in/caste/ugly-reality-caste-violence-discrimination-urban-india

[24]Kharbanda V and Hickok E.,MLATs and the proposed Amendments to the US Electronic Communications Privacy Act .https://cis-india.org/internet-governance/blog/mlats-and-the-proposed-amendments-to-the-us-electronic-communications-privacy-act

[25]The term "human rights" has been defined in the Act as "rights relating to life, liberty, equality and dignity of the individual guaranteed by the Constitution or embodied in the International Covenants and enforceable by courts in India".

International Covenants and enforceable by Courts in India.

**Practice:** Despite the existence of strong human rights standards in policy and law and adherence to international treaties, reports have called out human rights abuses that have taken place in India.[26]

**4. Governance and Oversight:** Legal mandates and procedures governing intelligence agencies and law enforcement authorized to seek data under the agreement. This includes procedures for collection, retention, use and sharing of data and oversight of the same.

Law and Policy: Intelligence agencies in India are not subject to oversight by Parliament[27], the Comptroller Auditor General of India[28], or the Right to Information Act 2005 except on questions of corruption and human rights violations.[29] The main provisions dealing with collection and sharing of data in criminal matters are enshrined in three different legislations, viz. (i) Section 69 of the Information Technology Act, 2000 ("**IT Act**") read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009; (ii) Section 5 of the Indian Telegraph Act, 1885 ("**Telegraph Act**") along with Rule 419A of the Indian Telegraph Rules, 1951; and (iii) section 91 of the Code of Criminal Procedure, 1973 (Cr.P.C.)[30] Rule 419A of the Indian Telegraph Rules provides for the establishment of review committees at the Central as well as State levels, which are to be responsible for overseeing requests for interception issued under the Act. The Central Committee shall consist of Secretaries to the Department of Legal Affairs as well as the Secretary to the Department of Telecommunications as members and the Cabinet Secretary as its Chairman. This same review committee oversees requests for interception, decryption, and monitoring issued under the Information Technology Act, 2000.[31] While the establishment of the Review Committee does give a semblance of oversight, the fact that it is comprised entirely of members of the Executive branch of government leaves much to be desired in terms of its independence. While the Review Committee oversees requests for interception and

[26] Roth K.( 2017).India Events of 2017.Retrieved from https://www.hrw.org/world-report/2018/country-chapters/india

[27] https://www.deccanherald.com/content/258689/time-parliamentary-oversight-over-intelligence.html

[28] https://timesofindia.indiatimes.com/india/Intelligence-agencies-cant-be-subject-to-CAG-audit-Centre-to-SC/articleshow/48550409.cms

[29] https://indianexpress.com/article/india/does-ib-have-to-provide-info-on-corruption-under-rti-delhi-high-court-asks-4979629/

[30] Although section 91 of the Cr.P.C. is an old provision which pre-dates the advent of the computer age and was perhaps drafted without keeping in mind requests for production of electronic data, however it is our understanding and experience that this provision is routinely used by the police to request information during an investigation.

[31] Vide Rule 2(q) of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

data issued under the Telegraph Act and the IT Act, it does not oversee requests issued under section 91 of the Cr.P.C. whereunder any officer in charge of a police station may order the production of information for the purposes of an investigation. The process of ordering the production of information under the Cr.P.C. currently has no oversight mechanism associated with it.

Practice: There is a lack of publicly available information regarding the implementation of these procedures. The Rules framed under the Indian Telegraph Act and the Information Technology Act create a procedure for collection, retention, use, and sharing of data. But whether these are adequate is to be determined. For example, the Rules under the Information Technology Act prohibit sharing of intercepted data by service providers but do allow for authorized agencies to share data for the purpose of investigation or in a judicial proceedings before the competent court. Our understanding of this is that this allows for sharing of data across cases - that evidence collected for one case - if relevant- can be used in another.[32] This is particularly true as India does not follow the doctrine of fruit from the poisonous tree.[33] Although the legal framework for interception and surveillance in India is laid out in legislations and incorporates authorization by an executive authority and review supervision by an "independent" body, there have been reports of surveillance that has been conducted outside this regime over the years.[34] Projects like the proposed Central Monitoring System have also been critiqued for threatening privacy and freedom of expression.[35]

5. **Accountability and Transparency (sub section v):** *Mechanisms to provide accountability and transparency regarding the collection and use of electronic data are also required.*

Law and Policy: Under the Information Technology Act and associated Rules, strict confidentiality is required to be maintained with regard to a direction for interception, monitoring or decryption.[36] Further the Telecom Licenses in India require that service providers maintain secrecy and confidentiality of any information disclosed for the purpose of implementing the licences.

---

[32]Rule 25 (3).The Information Technology Act Rules (2000).

[33] Bharat Chugh ( 2013, January 05).Telephone Tapping Constitutionality ? Whether illegal telephonic recording is admissible as evidence ?. Retrieved from https://bharatchugh.wordpress.com/tag/fruits-of-the-poisonous-tree-india/

[34] Aggarwal L.,Analysis of News Items and Cases on Surveillance and Digital Evidence in India.Retrieved from https://cis-india.org/internet-governance/blog/analysis-of-news-items-and-cases-on-surveillance-and-digital-evidence-in-india.pdf

[35] Litton, Addison. "The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression." Wash. U. Global Stud. L. Rev. 14 (2015): 799.

[36]Rule 25 (4).The Information Technology Act Rules (2000).

Practice: The stipulations of confidentiality have been interpreted by service providers as prohibiting transparency of any information related to interception requests including aggregate numbers. For example, Vodafone's Law Enforcement Report notes that any disclosure of lawful interception requests or requests for communication data would be unlawful.[37] As a distinction, Facebook, Google, and Microsoft report on takedown requests and user data requests in their transparency reports but not interception and communication content data requests.

**6. Commitment to an Open Internet (section vi):** *A demonstrated commitment to promote and protect the free flow of information across borders and open Internet.*

Law and Policy: In the last few years there has been a raging debate in academic circles on net neutrality in India. This debate moved to the mainstream in the backdrop of Facebook's famous "Facebook Zero" proposal. It was in this backdrop and as a result of the public debate that in 2016 the Telecom Regulatory Authority of India issued the Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016, that prohibit the practice of offering or charging discriminatory tariffs for data services based on content. Further, service providers are also prohibited from entering into arrangements that have the same effect as charging discriminatory tariffs on the basis of content. The two major themes incorporated in the Regulations may be said to demonstrate a commitment to promote and protect the free flow of information across borders and an open internet. India presently has data localization requirements in the Unified License[38] (for telecommunication service providers) and the Reserve Bank of India has required that all payment data must be stored within India.[39] The recent Data Protection Bill proposed by the Srikrishna Committee has clear data localization requirements - requiring copies of all personal data to be stored in India and all sensitive personal data to be stored within India. *If the Bill is enacted, these provisions along with existing data localization requirements will create a clear tension with the requirements found in the CLOUD Act.*[40]

**7. Minimization and Retention:** *The collection of data should be restricted to the amount needed for the purpose for which it is being collected and such data should not be retained for longer than is necessary*.
Law and Policy: As mentioned earlier, there are three main legislations used by

[37]Vodafone (2015).Law Enforcement Disclosure Report.Retrieved from https://www.vodafone.com/content/dam/vodafone-images/sustainability/downloads/54930_country_by_country.pdf
[38]Government of India Ministry of Communication & IT Department of Communications.License Agreement for Unified License.Retrieved from http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf
[39]Reserve Bank of India. Storage of Payment System Data.Retrieved from https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0
[40] Section 40 of the Personal Data Protection Bill. Reserve Bank of India.Storage of Payment System Data.Retrieved from https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0

enforcement agencies in India for surveillance and the collection of data, viz. The IT Act, the Telegraph Act and the Cr.P.C. There are no data minimisation and retention standards prescribed for an order under section 91 Cr.P.C., however the Rules under the IT Act as well as the Telegraph Act are discussed below:

(i) IT Act - As per the IT Rules[41] the competent authority must consider all alternate means of acquiring the information in arriving at its decision of issuing or approving an interception order. Further the IT Rules provide that all records, including electronic records, pertaining to interception must be destroyed by the government agency every six months, except when required for functional purposes. In addition, all records pertaining to directions for interception and monitoring are to be destroyed by the service provider within a period of two months following discontinuance of interception or monitoring, unless they are required for any ongoing investigation or legal proceedings.

(ii) Telegraph Act - Similar to the IT Rules, Rule 419A of the Telegraph Rules also provides that while issuing directions for interception the competent authority must determine if it is possible to obtain the information through other means. It also provides that records of directions for interception must be destroyed every six months by the relevant competent authority and the authorized security and law enforcement agencies, unless they are required for 'functional requirements'.

Practice: There is no publicly available information on how the provisions under the TA and ITA are implemented and no publicly available information on how much information is collected and stored under section 91 of the CrPc. That said, the big data boom has brought about the realisation that the value of data resides not in its primary purposes, but in its numerous secondary purposes, where data is reused many times over. This realisation is not limited to commercial businesses and can be found in the discourse around surveillance and envisioned projects in India. For example, the CCTNS, the NATGRID, and the Social Media Hub as well as plans for predictive policing are all projects that rely on collation and analysis of large quantities of data.

8. **Decryption Powers**: The terms of agreement will not require companies to decrypt information and will not prevent companies from decrypting data.

Law and Policy**:** The interception Rules under the ITA allow intelligence agencies to request the decryption of information and sharing of decryption keys. Though such powers exist in Indian law, intelligence agencies would be prohibited from evoking these under Indian law.

[41] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ("IT Rules").

Practice: There is no publicly available information about how this power has been evoked.

**9. Requirements of the Executive Agreement**

The other part of the Certification by the Attorney General requires him to certify that the Executive Agreement entered into between the United States and the foreign government (India) should contain specific safeguards which are listed below:

1. No direct or indirect intentional targeting of a US person.
2. The Indian government cannot issue an order on behalf of a third party government or share obtained information with the same.
3. An order issued by the Indian government must:
    a. be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;
    b. identify a specific person, account, address, or personal device, or any other specific identifier as the object of the order;
    c. in compliance with the domestic law of that country, and any obligation for a provider of an electronic communications service or a remote computing service to produce data shall derive solely from that law;
    d. be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation;
    e. be subject to review or oversight by a court, judge, magistrate, or other independent authority; and
    f. in the case of an order for the real time interception of wire or electronic communications, and any extensions thereof, shall require that the interception order—
        f.i. be for a fixed, limited duration
        f.ii. may not last longer than is reasonably necessary and must ensure that
        f.iii. it is issued only if the same information could not reasonably be obtained by another less intrusive method;
4. It is not used to infringe on freedom of speech;
5. Collected information is reviewed promptly and unreviewed information is stored on a secure system accessible only those persons trained in applicable procedures;
6. The Indian government shall, "using procedures that, to the maximum extent possible, meet the definition of minimization procedures in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)[42], segregate, seal, or

[42]50 USC 1801 War and National Defense. Retrieved from

delete, and not disseminate material found not to be information that is, or is necessary to understand or assess the importance of information that is, relevant to the prevention, detection, investigation, or prosecution of serious crime, including terrorism, or necessary to protect against a threat of death or serious bodily harm to any person;"

7. No disclosure of contents of communications of a US person to the US authorities except in certain circumstances and where it relates to significant harm, or the threat to the United States, including crimes involving national security such as terrorism, significant violent crime, child exploitation, etc.;
8. Reciprocal rights of data access must be granted to the United States.
9. There must be a periodic review of compliance by the Indian government with the terms of the agreement
10. The US government shall reserve the right to render the agreement inapplicable as to any order which it concludes the agreement may not be properly invoked.

The Act also permits data access when necessary for important reasons of public interest or for compelling legitimate interests when not overridden by the interest of the data subject, repetitive, and narrow in scope.[43]

On the above there may be two points of tension with Indian law and practice:

1. **Judicial Oversight:** Because the CLOUD Act will allow for local law to be applied if an Executive Agreement is entered into, India's regime of allowing executive authorization for interception requests technically falls within the framework defined by the Act, but it is not clear that this framework will meet the requirement of the domestic law provides robust substantive and procedural protections for privacy and civil liberties. This is particularly true as it has been noted by experts that the shift to a framework of judicial authorization by the U.K in 2016 was motivated by the need to meet the conditions necessary for an executive agreement.[44] Though in some contexts with robust judicial systems - this standard could be considered a point of weakness in the Act, given the problems that have been alleged[45] to beset India's judicial regime including corruption and an overburdening[46] of the system, it is less controversial for orders to be approved

---

http://uscode.house.gov/view.xhtml?req=(title:50%20section:1801%20edition:prelim)

[43]Daskal J., (2018, May). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.Retrieved from https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/

[44] Nojeim G., (2018, July 10).Cloud Act Implementation Issues.Retrieved from https://www.lawfareblog.com/cloud-act-implementation-issues

[45]Livemint. Corruption Catalogues. Retrieved from https://www.livemint.com/r/LiveMint/Period1/oldpdf/8f771b83-547a-4758-ba01-0c2c57b70065.pdf

[46]Business Today. (2018, June 28) 3.3 crore cases pending in Indian courts, pendency figure at its highest: CJI Dipak Misra. Retrieved from https://www.businesstoday.in/current/economy-politics/3-3-crore-cases-pending-indian-courts-pendency-figure-highest-cji-dipak-misra/story/279664.html

by the executive and principles such as impartiality and independence become more critical to ensuring that requests are necessary and proportionate.

2. **Freedom of Expression:** Though Article 19 of the Indian Constitution upholds freedom of expression, India has a history of actions that have challenged freedom of expression with concerns that this is on an increase.[47] In particular, the number of network shutdowns that have been ordered in India have raised concerns from both the national and international community.[48]

**Evolution of the CLOUD Act**

The CLOUD Act is a reaction to the need for better cooperation between governments of different countries in the age of the internet. However, as mentioned earlier, the CLOUD Act is not the first effort in this regard, it is no surprise that there have been other efforts in the past to address this concern, and the CLOUD Act builds upon the suggestions and processes put forth by such proposals. The first such proposal, which the CLOUD Act follows closely, was made by the U.S. Department of Justice in July, 2016 in which amendments were proposed to the Electronic Communications Privacy Act (the "**DOJ Bill**"). In order to understand how the legislation has evolved, we compared the DoJ Bill with the CLOUD Act. The two main differences we found between the DOJ Bill and the CLOUD Act are:

- **Judicial Challenge to Data Requests and Immunity for good faith disclosures**: The CLOUD Act gives U.S. data services providers who have been served with a request from a governmental entity in the U.S. seeking data stored in a country with which the U.S. has an Executive Agreement the ability to approach the Court to modify or quash such an order, if it reasonably believes: (1) the customer or subscriber is not a U.S. person and does not reside in the United States, and (2) the required disclosure would create a material risk of violating the laws of a qualifying foreign government. The Act also provides that the Court may grant such an application if it finds that the disclosure would violate the foreign government's law; and the interests of justice dictate that the legal process should be modified or quashed. Though we feel that this is an important safeguard and

[47]Prabhu M., (2017, August 03). Is free speech under threat in Modi's India? Retrieved from https://www.aljazeera.com/indepth/features/2017/07/free-speech-threat-modi-india-170712131837718.html and Roy S., (2017, May 02). For India, a Year of Shrinking Freedom of Speech. Retrieved from https://thewire.in/politics/for-india-a-year-of-shrinking-liberty

[48] Internet Shutdowns, SFLC.in Retrieved from https://www.internetshutdowns.in/ and The Economic Times (2017, May 13).India witnessed highest number of internet shutdowns in 2017-18 UNESCO report. Retrieved from https://economictimes.indiatimes.com/tech/internet/india-witnessed-highest-number-of-internet-shutdowns-in-2017-18-unesco-report/articleshow/64150543.cms, and BBC (2017, June 16). India internet shutdowns'violate 'human rights.Retrieved from https://www.bbc.com/news/world-asia-india-40298722

provides companies with a clear mechanism to push back against requests - it is unclear how companies will be accountable for the decisions they take. There is a risk that the immunity from actions for good faith disclosures will act as a blanket shield for any decision taken by a company. The CLOUD Act purposefully outsources a function that was traditionally undertaken and formally deliberated upon by a court - to the private sector. In doing so, companies need to be held accountable for their actions as they continue to grow as gatekeepers for users' rights. Will individuals be able to challenge compliance with requests? Come to know about compliance? Will companies share insights into their decision making process?

- **Attorney General's Certification regarding adequacy of Foreign Law:** the CLOUD Act requires that the Attorney General should certify to the U.S. Congress that the legal framework of the foreign government "affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities". The Act then lists out the eight factors that have "to be met" for the Attorney General to arrive at such a determination. The DOJ Bill used the phrase "factors to be considered" and not "factors to be met". It appears that this change in drafting was brought about to strengthen the requirements that the foreign law has to satisfy in order to qualify under the CLOUD Act, in that all the factors mentioned in Title 18 § 2523 (b)(1)(B) have to be satisfied for the Attorney General to be able to give his certification, as opposed to such factors merely being considered for the purposes of the certification. We see this as a positive step as it provides more clarity on what requirements a foreign law will have to meet - though there is still uncertainty in the implementation of the Act.

**Perspectives on the CLOUD Act**

Reactions to the CLOUD Act have been mixed. On one hand, there has been support for the Act - noting that it is an important step forward towards addressing the challenges associated with cross border sharing of data and that it supports privacy and civil liberties while building in accountability mechanisms[49], while others have criticized the Act as globally lowering the bar for access to content data. Some of the major criticisms are given below:

*Executive Nature:* The fact that the agreements will be executive without clear approval by Congress has been pointed out as a weakness in the Act and potentially will allow for agreements to be entered with countries that do not have a strong record of respecting

[49]Swire P and Daskal J.Lawfare (2018, March 14).Why the CLOUD Act is Good for Privacy and Human Rights. Retrieved from https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights

and upholding human rights.[50]

*Opacity in Introduction:* The CLOUD Act has been criticized for being quickly introduced as part of a Omnibus Spending Bill without extensive public consultation or consultation with foreign policy makers. Beyond criticizing the process as being non-transparent, experts, notably from the EU, have highlighted that the process followed for enacted the CLOUD Act has narrowed the possibility for solutions to be agreed upon between the EU and US.[51]

*Lack of Judicial Authorisation*: The CLOUD Act requires that the "qualifying foreign governments" have a process whereby a person could seek post-disclosure review by an independent entity (in the case of India, this would be the Review Committee established under Rule 419A of the Telegraph Rules) instead of a warrant by a court. Although a court order is not the norm for interception even in Indian law, under American law such protection is given to data held by American companies even though the data may belong to Indian citizens.[52]

*Disclosure without a Warrant based on probable cause*: Under the MLAT framework, any request to the US would be subject to US law meaning a judge in the U.S. must issue a warrant based on probable cause in order for a U.S. company to turn over content to a foreign government. This requirement has been seen as often offering a higher level of protection to individuals abroad by requiring that their governments' MLAT requests meet certain standards when seeking information held by U.S. companies. This would be the case for India and countries with similar frameworks. The CLOUD Act does not include this essential safeguard for a warrant based on probable cause and allows foreign governments under an Executive Agreement to issue requests as per local law. Civil Society in the US including the Center for Democracy and Technology and the Electronic Frontier Foundation have voiced concern over this lowering of standards noting that it weakens and erodes user privacy protections.[53]

---

[50]ACLU.Coalition Letter on Cloud Act" Retrieved from https://www.aclu.org/letter/coalition-letter-cloud-act

[51]EUobserver (2018, August 21).Rushed US Cloud Act triggers EU backlash. Retrieved from https://euobserver.com/justice/141446

[52]Kharbanda V and Hickok E., The Centre for Internet and Society (2016, October 20).MLATs and the proposed Amendments to the US Electronic Communications Privacy Act. Retrieved from https://cis-india.org/internet-governance/blog/mlats-and-the-proposed-amendments-to-the-us-electronic-communications-privacy-act

[53]Cdt (2018, February 06).CLOUD Act Would Erode Trust in Privacy of Cloud Storage. Retrieved from https://cdt.org/press/cloud-act-would-erode-trust-in-privacy-of-cloud-storage/ and Fischer C.,EFF (2018, February 08).The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data. Retrieved from https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-

*Vague Standard for Requests*: Under the domestic law of any state there is usually a large amount of jurisprudence regarding when search orders can be issued, such as the "probable cause" standard that is followed in the United States or similar standards that may be followed in other jurisdictions. This ensures that even when the wording of the law is not precise, which it cannot be for such a subjective issue, there is still some amount of clarity around when and under what circumstances such warrants may be issued. In contrast, the CLOUD Act requires that orders be based on "requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation." Although the language here may seem reasonable, in the absence of any jurisprudence backing it, it becomes very vague and susceptible to misuse.

*Limited grounds for judicial oversight*: While the CLOUD Act provides a mechanism of judicial oversight, it appears unlikely to be an effective method of protecting the privacy of individuals. The Act provides that the service provider which has received a request for data from a U.S. law enforcement agency may challenge such a notice in a court of law on the grounds that (i) the person who is the subject of the request is not a United States citizen; and (ii) such disclosure would cause a material risk of the service provider violating the laws of the foreign government. Thus the only ground on which the service provider is allowed to challenge the order is that it would put the service provider at risk of violating the privacy laws of the relevant jurisdiction; therefore it could become an exception to safeguard the service providers from legal liability in a foreign jurisdiction rather than a provision to enforce the privacy rights of the subjects of the disclosure order.[54]

**Conclusion**

As a result of the broad language used in the Act, the impact will largely be shaped by implementation. Greg Nojeim, Director of the Freedom, Security & Technology Project at the Center for Democracy and Technology, has called out eleven issues[55] that can arise in the implementation of the CLOUD Act. These include:

1) If the DoJ will continue to issue warrants to obtain data of foreigners,
2) If the Act will address data disclosed in death penalty cases,
3) If judicial authorization will be required,

---

cross-border-data

[54]Fischer C.,EFF (2018, February 08).The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data. Retrieved from https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data

[55]Nojeim G., Lawfare (2018, July 10)."Cloud Act Implementation Issues."Retrieved from https://www.lawfareblog.com/cloud-act-implementation-issues

4) The extent to which the government will be transparent about agreements entered into,
5) The extent to which the agreements will require foreign countries to allow company transparency on requests,
6) Which standards of freedom of expression will be applicable,
7) If companies will be allowed to notify the US government of problematic data requests,
8) Whether the US government can suspend data arrangements under an agreement when a government undergoes significant changes
9) If agreements will ensure that data demands meet the criteria of the MLAT or the CLOUD Act.
10) If clear points of contact within a country will be established, and
11) If there will be consultation with human rights experts.

Of the above, the questions on death penalty, free speech standards, judicial authorization, transparency of requests, and consultation with human rights experts will be particularly important for India to have clarity on.

For India, the scope of laws and policy taken into consideration, the criteria needed to fulfill certain requirements, the weight attached to practice vs. existence of a policy, the timeframe for assessing practice, the materials relied upon, and the experts consulted will play a role in the outcome of the determination. From our evaluation above, it could be considered that India's legal regime for access to stored content data is lacking compared to the CLOUD Act requirements. In particular, the data requests for content data sent under section 91 Cr.P.C. do not appear to satisfy the CLOUD Act requirements and could present a significant hurdle for certifying Indian laws as adequate. On the other hand, the legal regime around interception would come closer to being considered adequate - though the transparency requirements in the CLOUD Act are not met. It is not clear if the Supreme Court's recognition of the right to privacy would be considered sufficient or if the Act would also require that India have in place a comprehensive data protection legislation. Current data localization requirements in the finance and telecom sector could also hinder such an assessment. Similarly, the lack of accountability for intelligence agencies in India could be another hurdle. With respect to practice - this is a harder determination to take a clear stance as we (the authors) have only publicly available information to rely on. India's practices around content restrictions and network shutdowns, legal adherence to the legal regime for surveillance, respect for human rights, concerns around discrimination, and challenges with the judicial system - will all need to be taken into consideration.

It is unclear from the wording of the CLOUD Act as it stands now, if a positive assessment will require fundamental changes in Indian law or if it will create a framework for cross border sharing of information that is grounded in Indian law but sits on top of the existing

framework. This is important to note because if India is offered an agreement without requiring any changes to this legal mechanism, it could allow the Government of India to access stored content data from US companies at a much lower standard than currently is required under the MLAT system as per U.S standards. On the other hand, the CLOUD Act could catalyze some welcome changes to India's surveillance regime - such as allowing transparency of requests and strengthening the safeguards around access to stored content data. There are other areas of India's surveillance regime that the CLOUD Act may not impact - one being the disproportionate penalty of seven years in prison and a fine for non-compliance with interception, monitoring, and decryption orders.

It will be interesting to see if, just as the US will have the ability to ask India to be reviewed for compliance with the Act, if India can request the US to be reviewed for compliance with the Act and on what terms. It will also be interesting to see how the reciprocal nature of the agreement plays out - will the US be held to the same standards of data access as India.

The CLOUD Act has the potential to address some of the issues with the MLAT system - such as duration to respond to requests and differing standards between Indian and US law. At the same time, some of the identified issues with the India-US MLAT system are process oriented - including capacity deficits, process delays, and differing policies from service provider to service provider[56] could potentially carry over to a new framework.

In her article for the Stanford Law Review, Jennifer Daskal, Associate Professor at George Washington University, notes that the CLOUD Act and the GDPR are examples of international lawmaking done via domestic regulation. This is in contrast to the traditional process of global treaties and agreements reached through consensus and consent.[57] In light of the failed GGE, and as the global community struggles to establish a framework to govern cyberspace, it will be interesting to see the role that this new form of international lawmaking will play in the long run and how non EU or US countries will respond. A question policy makers in India need to reflect on is 1. If an agreement like the CLOUD Act is desirable 2. and if so, what changes will be necessary to enter into an executive agreement.

---

[56] Mohanty B and Srikumar M., ORF Special Report (2017, August). Hitting Refresh - Making India -US Data Sharing Work.Retrieved from https://www.orfonline.org/wp-content/uploads/2017/08/MLAT-Book.pdf

[57] Daskal J., (2018, May), Microsoft Ireland, the CLOUD Act, and International Lawmaking 2. Retrieved from https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/