AICYBERLEX NEXUS

Journal of Artificial Intelligence, Cyber & Contemporary Law

Volume I · **Issue I** · **Jul–Sep 2026** · Article 4
ISSN: Applied for (National ISSN Centre, NIScPR, India) · e-ISSN: TBA
Peer-reviewed · Open Access · https://aicyberlexnexus.com

ARTICLE 4

Evidence Across Borders: The Limits of MLAT Cooperation in Cybercrime Investigation

Sunandha

ABSTRACT

Almost every serious cyber-crime investigation in India sooner or later needs something held abroad: the subscriber details behind an account, the content of a message, the logs of a server. The main formal route for getting such material is a request under a mutual legal assistance treaty, and it is widely regarded as too slow for data that can be deleted in minutes. This paper explains how cross-border evidence is sought under Indian law, why the treaty route struggles with digital material, and what the alternatives are, including direct requests to companies, the American CLOUD Act, the Budapest Convention and its Second Additional Protocol, and the new United Nations cybercrime convention. It argues that India should pursue a layered approach: keep the treaty route for serious and contested cases, build faster channels for basic subscriber and log data, and invest in domestic capacity to make requests that foreign authorities can act on.

KEYWORDS: cybercrime; mutual legal assistance; electronic evidence; jurisdiction; CLOUD Act; Budapest Convention

1. Introduction

A police officer in Pune receives a complaint. A woman has been blackmailed with intimate images sent from an anonymous account on a foreign messaging service. The account holder's details are stored on servers in another country. The officer knows who holds the key but has no power to walk in and demand it. This is the ordinary shape of a modern cyber-crime case. The victim is in India, the offender may be anywhere, and the evidence sits with a company whose servers, staff and legal department are in a third place. Criminal procedure, however, was built on territory. A court's summons runs inside the country's borders, and evidence abroad is reached through diplomacy. The diplomatic route is the mutual legal assistance treaty, or MLAT. It served well when the evidence was a bank ledger or a witness statement. It copes badly with data that can vanish quickly, that is held by private companies and that is mixed with the data of thousands of other users. The paper has six parts. Part 2 describes the present Indian framework. Part 3 explains why MLATs struggle. Part 4 looks at alternatives. Part 5 proposes a way forward for India, and Part 6 concludes.

2. How cross-border evidence is sought today

2.1 Letters of request

1

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) provides for requests for evidence abroad. Where a court or investigating officer in India needs evidence from a country with which reciprocal arrangements exist, a letter of request can be issued to the court or authority in that country, and the BNSS also deals with requests that come in from abroad. These provisions replaced section 166A and related sections of the old Code of Criminal Procedure.[1] The request is normally routed through the Ministry of Home Affairs, which acts as India's central authority for mutual legal assistance in criminal matters, and then through diplomatic channels or the foreign authority named in the treaty. 2.2 Treaties India has mutual legal assistance treaties in criminal matters with a few dozen countries, including the United States, whose treaty was signed in 2001 and entered into force in 2005. Where no treaty exists, requests proceed on the basis of reciprocity or through letters rogatory, which rely on comity and are slower still. 2.3 The Indian side of data requests Within India, the powers to compel data are better developed. Section 94 of the BNSS lets a court or police officer require production of documents and things. Section 69 of the Information Technology Act, 2000 and the 2009 interception rules provide for interception, monitoring and decryption on stated grounds, and the Act applies to offences committed outside India that involve a computer system in India.[2] The difficulty is that a notice to a foreign company with no Indian presence has little force, and even companies with Indian subsidiaries often say that the data is controlled elsewhere.

3. Why MLATs struggle with digital evidence

Several reasons recur in the literature and in the experience of investigators. Time is the first. A request must be drafted, reviewed, sent through ministries, examined by the foreign central authority, taken to a court in the other country, and then served on the company. Reviews of the American system, which receives the largest number of foreign requests because so many major platforms are based there, have described delays measured in months.[3] Many service providers retain some logs for only a limited period, so by the time the request arrives the data may be gone. The second reason is volume. Foreign central authorities were never staffed for the flood of requests that internet services produce. Each request, however minor, has traditionally required the same formal steps as a murder inquiry. The third is legal mismatch. A requesting state must satisfy the other country's standard, which in the United States means showing probable cause for content. Indian requests drafted in the style of a domestic notice often fall short and come back for more information, which adds more months. The fourth is the uncertainty over where data is. Cloud storage splits and moves data across borders. In United States v Microsoft Corp, an American case on emails stored in Ireland, the

2

question of whether a warrant could reach data held abroad by an American company went all the way to the Supreme Court before Congress passed a statute that made the dispute moot.[4] If wealthy states struggle to say where data "is", the difficulty for a district-level Indian investigating officer is plain. The fifth is capacity at home. Poorly framed requests, missing certificates under the electronic evidence rules, and unclear chain of custody can make material unusable even when it arrives.

4. Alternatives to the treaty route

4.1 Voluntary disclosure by companies Many large platforms respond to direct requests from Indian law enforcement, especially for subscriber information and in emergencies involving threats to life. Transparency reports show that these requests are common and often at least partly granted. This route is fast, but it rests on corporate policy rather than law. It can change with a company's mood, it gives courts no say, and it is least reliable in the contested cases where it is most needed. 4.2 The CLOUD Act and executive agreements The American Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018 confirmed that American providers must produce data in their "possession, custody or control" wherever stored, and allowed the United States to enter into executive agreements with qualifying foreign governments, letting their authorities send orders directly to American companies.[5] The first such agreement was with the United Kingdom. Qualifying requires the partner country to meet rule-of-law, privacy and procedural standards, which presents a challenge for any country whose interception regime lacks judicial authorisation. India has reportedly explored such an arrangement, but any agreement would require a closer look at India's own safeguards. 4.3 The Budapest Convention and its protocol The Council of Europe's Convention on Cybercrime of 2001 gives parties common offences, procedural powers such as expedited preservation of data, and a framework for cooperation, including a network of 24/7 contact points. India has not joined, historically citing the fact that it did not take part in drafting and concerns about sovereignty. The Second Additional Protocol of 2022 goes further, setting up direct requests to providers for subscriber information and fast-track mechanisms for emergencies.[6] Non-members can learn from it even if they stay outside. 4.4 The United Nations convention In December 2024 the UN General Assembly adopted a Convention against Cybercrime, designed to provide a universal framework for criminalisation and cooperation, and it was opened for signature in 2025.[7] Supporters value its reach, since it is not limited to a regional club. Civil-society groups have criticised it for weak human rights safeguards and a broad scope covering any serious crime committed through technology. Whether India joins, and with what reservations, is a policy decision that will affect how it can cooperate.

5. A way forward for India

3

The central point is that no single channel will serve all cases. A sensible system keeps different tools for different needs. For serious offences and contested evidence, the treaty route should stay, but it needs repair. The Ministry of Home Affairs could set up a dedicated unit for digital requests with standard templates matching the legal tests of the main destination countries, and track each request's status so that officers know where their file is. Agreed model forms with the United States would save months. For basic subscriber data and logs, India should negotiate faster channels. This could take the form of a CLOUD Act agreement, a protocol-style arrangement with partners, or clear written rules for direct requests to providers with an Indian presence. Any such channel should come with independent oversight, because speed without safeguards is its own danger. The Supreme Court's reasoning in Puttaswamy requires legality, necessity and proportionality for intrusions on privacy, and a data-access regime that lacks judicial or independent review would sit uncomfortably with it.[8] Preservation should be separated from production. An officer should be able to ask a company quickly to freeze data while the formal request travels. The Budapest model of expedited preservation does exactly this, and it requires little more than a clear statutory power and a point of contact. Domestic capacity matters too. Police, prosecutors and judges need

training in how to frame an international request, what a foreign authority needs to see, and how to meet the certificate and authenticity requirements for electronic records so that the evidence stands up in an Indian trial. Finally, India should decide, after open debate, whether to join one or more of the multilateral frameworks. Staying outside keeps flexibility but costs speed. Joining brings obligations on rights and procedure that domestic law would have to meet.

6. Conclusion

The mutual legal assistance treaty is a tool of its age. It was designed for paper records and slow diplomacy, and it is poorly matched to data that moves in seconds and sits with private companies. No replacement is perfect: voluntary disclosure is unreliable, the CLOUD Act route demands high safeguards, and the multilateral conventions bring trade-offs. India's best course is a layered one — a repaired treaty channel for serious matters, faster and supervised channels for routine data, quick preservation powers and trained investigators. A victim in Pune should not have to wait many months because the evidence is on a server abroad.

References [1] Bharatiya Nagarik Suraksha Sanhita 2023, Chapter VIII (reciprocal arrangements for assistance in certain matters) and s 94; compare Code of Criminal Procedure 1973, ss 105A-105L and s 166A (repealed). [2] Information Technology Act 2000, ss 69, 75; Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009.

4

[3] President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World (2013), on the duration of MLAT requests. [4] United States v Microsoft Corp 584 US ___ (2018) (per curiam; dismissed as moot after the CLOUD Act). [5] Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub L 115-141, div V (2018). [6] Council of Europe, Convention on Cybercrime (ETS No 185, 2001); Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence (CETS No 224, 2022). [7] United Nations Convention against Cybercrime, adopted by the General Assembly on 24 December 2024. [8] Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

5

Cite as: Sunandha, “Evidence Across Borders: The Limits of MLAT Cooperation in Cybercrime Investigation”, *AICyberLex Nexus*, Vol. I, Issue I, Jul–Sep 2026, Article 4. Available at https://aicyberlexnexus.com
© 2026 AICyberLex Nexus. Open access under the terms stated on the journal website.