Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
May 2024 5(5), 1185–1190

ADDRESSING CROSS- BORDER DATA ACCESS FOR EFFECTIVE LAW ENFORCEMENT

Shruti Das[1], Dr. Sarika Sagar[2]

[1] Department of Law, Vishwakarma University, Pune, Maharashtra, India

DOI
10.29121/shodhkosh.v5.i5.2024.2861

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Online data is increasingly used by law enforcement to obtain evidence for investigations. Accessing this data, especially from cloud-based services, is difficult due to jurisdictional issues and changing technology. This article examines how cloud computing, data protection legislation, and multinational collaboration affect law enforcement agencies' cross-border data access. Extraterritorial data access legislation in the U.S. and EU pose accountability and transparency concerns, especially in liberal democracies. The study discusses private sector monitoring, corporate social responsibility programs including transparency reports, and state-corporate surveillance issues. In India, law enforcement agencies increasingly use cross-border data access but struggle with delayed and complicated mutual legal assistance treaties (MLATs) and Letters Rogatory (LRs). Tech company transparency reports show that data disclosure policies and regulatory requirements vary, with India failing to get vital evidence. The article continues by examining India's emerging data governance structure, including privacy, cross-border transfers, and law enforcement access issues. To secure data governance and security in an increasingly linked world, clearer legislation, increased international cooperation, and global best practices are needed

1. INTRODUCTION

Law enforcement agencies increasingly rely on online data for evidence collection, as both cyber and non-cybercrimes now often involve online activities. A 2018 European Commission report indicated that 85% of investigations require electronic evidence. However, technology advancements, especially cloud computing, present challenges in accessing this evidence, leading both the U.S. and EU to enact extraterritorial data access laws. This cross-border access raises concerns around accountability and transparency, which are fundamental to liberal democracies yet often lack clarity and openness in practice.

Cloud computing also impacts other fields, including economics, cybersecurity, digital rights, and data protection, while influencing geopolitical rivalries. Europe, for instance, is exploring sovereign cloud solutions to reduce dependency on other countries, which complicates traditional territorial-based jurisdictions.[1]

Additionally, private sector surveillance—highlighted by Snowden's revelations—connects closely with state surveillance, leading to discussions on "surveillance capitalism," where companies profit from personal data. Although European data protection efforts aim to shield citizens from corporate surveillance, state surveillance is also growing in response to cybercrime and terrorism, thus reducing data protection scrutiny for LEAs.[2]

[1] Harfield, C. (2003). A Review Essay on Models of Mutual Legal Assistance: Political Perspectives on International Law Enforcement Cooperation Treaties. International Journal of Comparative and Applied Criminal Justice, 27 (2), 221–241
[2] Fennelly, D. (2019). Data Retention: The Life, Death and Afterlife of a Directive. ERA Forum, 19 , 673–692.

In response, some companies publish transparency reports to show data requests from LEAs and intelligence agencies, aligning with corporate social responsibility principles. This practice offers a partial view of data sharing, though secrecy around surveillance complicates understanding what data is collected. Definitions around "evidence" and "data" are unclear, especially with metadata like IP addresses and GPS location data. Legal protections for data types vary, and the evolving technologies complicate distinctions between data in transit and at rest, sparking calls for better data classification in global jurisdictions. [3] This study thus examines how tech companies categorize data in transparency reports, alongside observations on their legal practices.

2. CUSTOMARY PRACTICES OF CROSS-BORDER DATA ACCESS

Law enforcement agencies use multiple methods to access online data for investigations and predictive analysis. A significant amount of data is publicly available online, allowing agencies to gather open-source intelligence on public sentiment, harmful content, hate speech, and misinformation. However, proprietary data held by private companies requires more complex access methods. In the U.S., agencies have historically used four approaches: direct corporate agreements, letters rogatory, law enforcement collaboration, and mutual legal assistance treaties (MLATs). Direct requests to tech firms, especially those based in the U.S., have become common but raise issues around accountability, privacy, and human rights, as companies often lack resources to assess privacy implications thoroughly.[4]

Letters rogatory involve formal international judicial assistance but are inefficient and rarely used, with law enforcement agencies more frequently relying on collaboration and MLATs. International collaboration allows agencies to share data through agreements with organizations like INTERPOL and EUROPOL. Meanwhile, the MLAT system, though established to respect national sovereignties, is criticized as slow and bureaucratic, often causing delays in accessing electronic evidence, especially when cooperation involves the U.S.[5]

The MLAT system also relies on dual criminality, complicating matters for crimes with differing legal definitions across borders. Consequently, due to the inefficiencies of MLATs, European law enforcement increasingly turns to direct requests to U.S. tech firms, though these practices raise concerns about transparency, data protection, and sovereignty.[6]

3. INDIA'S PRACTICE OF CROSS BORDER DATA ACCESS:

In India, the average internet user consumes around 10.40 GB of wireless data each month for activities like communication, entertainment, and accessing information. As more personal and business interactions shift online, the government's interest in understanding these digital exchanges has grown. Detailed knowledge of these transactions can support the state in crafting better policies, ensuring regulatory compliance, and more effectively performing law enforcement duties. This discussion focuses on data access specifically for law enforcement purposes.

The cross-border nature of digital activities heavily impacts authorities' ability to access data for law enforcement, especially when data controllers or storage locations lie outside national borders. The European Commission estimates that electronic evidence is involved in roughly 85% of criminal investigations, with two-thirds involving service providers in other jurisdictions. Although no comparable data is available for India, service provider transparency reports reveal a growing role of digital data in criminal cases. For instance, Facebook received 49,382 information requests from India in 2019, a figure that tripled since 2016. Similar trends are evident in reports from Google and Twitter, reflecting the rapid growth in India's internet users over recent years, leading to a higher volume of digital transactions, many with international components.

Cross-border data access requests are guided by the laws in both the requesting country and the jurisdiction of the service provider or data storage site. Often, these laws limit access to personal data by third parties, including foreign governments. In such cases, mutual legal assistance treaties (MLATs) are typically used. By November 2019, India had

[3] Daskal, J. (2016). Law Enforcement Access to Data across Borders: The Evolving Security and Rights Issues. Journal of National Security Law & Policy, 8 (3), 473–501.

[4] Daskal, J., & Swire, P. (2018a). A Possible EU-US Agreement on Law Enforcement Access to Data? (Lawfare Blog. Available online in January 2013: https://www.lawfareblog.com/possible-eu-us-agreement-law -enforcement-access-data)

[5] de Hert, P., & Aguinaldo, A. (2019). A Leading Role for the EU in Drafting Criminal Law Powers? Use of the Council of Europe for Policy Laundering. New Journal of European Criminal Law, 10 (2), 99–106.

[6] Ibid

signed MLATs with 42 countries and six international treaties with mutual legal assistance provisions. However, MLATs are frequently criticized for being slow, complex, and lacking robust data protection. As a result, policymakers continue exploring alternative methods for data access in law enforcement, making it a central issue in policy discussions.

Indian law enforcement agencies commonly rely on Section 91 of the Criminal Procedure Code (CrPC) to access any "document or other thing" deemed necessary for an investigation, either through a summons issued by the court or a directive from the police officer in charge. Additionally, under the Indian Telegraph Act of 1885 and the Information Technology Act of 2000, these agencies can request message interception or data disclosure. Despite its age, the Telegraph Act imposes a slightly higher legal threshold for data access. In December 2018, the government listed ten investigative and security agencies, including the Intelligence Bureau, Narcotics Bureau, and Enforcement Directorate, authorized to request data interception, monitoring, and decryption under the IT Act.[7]

Another avenue for cross-border data access is through Letters Rogatory, which are formal requests from the judiciary of one country to another for assistance in criminal investigations or prosecutions. In India, procedures for issuing a Letter Rogatory are outlined in Sections 166A and 105K of the CrPC, along with Sections 57 and 61 of the Prevention of Money Laundering Act, 2002 (PMLA) and Section 12 of the Fugitive Economic Offenders Act, 2018 (FEOA). These provisions enable an investigating officer to request aid via a competent court. Handling requests from foreign courts or authorities follows guidelines established in Sections 166B and 105K of the CrPC and Section 58 of the PMLA, among others. Letters Rogatory facilitate the service of documents and evidence collection, and they may be issued based on bilateral or multilateral treaties, international conventions, or reciprocal assurances. All Letters Rogatory drafts require the Central Authority's (IS-II Division, MHA) approval. Requests are only submitted to the Court for issuance following MHA concurrence.[8]

The Letters Rogatory process follows several sequential steps under various legal provisions, including Sections 166A and 105K of the CrPC, Chapter VII A of the CrPC, Sections 57 and 61 of the PMLA, and Section 12 of the FEOA:

1. Request Initiation by Investigating Officer (IO) or Agency: The Investigating Officer drafts the request, compiling case-related details and specifying the assistance needed from the foreign country. Legal opinion or recommendations from the Director of Prosecution (DOP) are obtained, followed by formal approval from the Director/Director General for central investigating agencies, relevant Ministry for central agencies, or the State Government for state-level matters.
2. Request Transmission to the Central Authority (IS-II Division, Ministry of Home Affairs - MHA): If initiated by State Police, the request draft goes through the State's Home Department to the Central Authority. For Central Agencies, the draft is sent directly to the Central Authority after obtaining approval from the respective Ministry or Head of Department.
3. Review by the IS-II Division (MHA - Central Authority of India): Upon receiving the draft, the IS-II Division evaluates the request and may (i) approve it, allowing the Investigating Agency or State Government/UT to proceed to Court for issuance, (ii) return the draft for further clarification or modification, or (iii) reject the request if it doesn't meet necessary standards.
4. Authorization and Judicial Issuance: After obtaining MHA's concurrence, the request can be submitted to the Court for issuing the Letters Rogatory. All requests must route through the IS-II Division before reaching the Court.
5. Consultation (if required): The Central Authority (IS-II Division) may directly engage with a representative from the Investigating Agency for further clarification as necessary.

4. CASE STUDIES

The dataset compiled from transparency reports by technology firms offers various quantitative insights, focusing on requests made by law enforcement agencies (LEAs) for archived web data. These transparency reports, based on information from 71 companies and compiled with the help of the Access Now transparency index, span a range of companies, mostly from the United States, with others located in Europe, Canada, New Zealand, and other regions. Many of these companies are categorized as internet and mobile ecosystem providers, with 15 telecommunications companies and two exceptional cases.[9]

[7] https://www.mha.gov.in/en/commoncontent/mutual-legal-assistancemla-criminal-matters

[8] https://www.mha.gov.in/en/commoncontent/mutual-legal-assistancemla-criminal-matters

[9]Access Now (2023). Transparency Reporting Index. (Available online in January: https://www.accessnow.org/transparency-reporting-index/)

The transparency reports cover data from the past three years and reveal that 64 companies provided quantitative data on LEA requests. The number of requests made by LEAs to these companies is shown in Figure 1, with both domestic and international inquiries included. These requests often involve emergency requests and preservation orders, but requests for material bans or copyright takedowns are excluded. Requests from intelligence agencies, particularly in the United States and some other nations, are also included. However, some corporations do not disclose intelligence-related requests due to legal restrictions in their home countries, particularly with regard to national security.[10]

The analysis suggests that law enforcement agencies often seek data from telecommunications companies, with Vodafone, Telia, and T-Mobile being the top three most requested companies. Other telecommunications firms such as Telefónica, AT&T, Rogers, and Verizon are also frequently contacted. This finding contrasts with European polls suggesting that companies like Google, Facebook, and Microsoft were the most contacted entities by European law enforcement (EUROPOL, 2020). These findings raise concerns about the overemphasis on cloud computing in existing literature, particularly when examining law enforcement's data access practices.[11]

The transparency reports also highlight the data release procedures of the companies. Approximately 69% of the companies require a formal court process before disclosing data, though some may voluntarily release data if they deem the request legitimate. About 42% of companies have specific procedures for international requests, often referencing Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory, while some mention bilateral agreements under the CLOUD Act. This limited regulation for cross-border requests suggests that law enforcement still resorts to direct requests, bypassing formal legal channels.[12]

Additionally, 48% of the companies try to inform users about LEA requests, except in cases involving gag orders, emergency situations, or sensitive matters like the sale of harmful substances. The reports also provide insight into the types of data disclosed. Around 31% of the companies fail to disclose the specific data they share in response to LEA requests, while 20% describe the release of content data based on user accounts. Some companies, such as those with no-logs policies, claim they do not retain non-content data, when they receive requests for genetic data from law enforcement, despite the sensitive nature of this information under the GDPR.[13]

The companies can be grouped based on the types of data they disclose in response to LEA requests. One group, including prominent firms like Amazon, Cisco, and Facebook, distinguishes between content and non-content data. For example, Amazon classifies subscriber information as non-content data, while designating information stored on its cloud service as content data. Other companies, like Comcast and Zoom, also categorize data based on communication content and metadata. Apple, Uber, and Xiaomi fall into a fourth group, with data categories that include device and vehicle information, financial identity data, and user account content data. These companies do not provide specifics on the device data, leaving some ambiguity about the nature of the data they disclose.[14]

The final group consists of telecommunications firms and companies offering internet and mobile ecosystems, which often provide wiretap data for communications. These firms may also allow real-time interception of communication content in line with national laws. The data types and classifications within this group vary, with companies like Telefónica and Telia distinguishing between content data and metadata and clarifying their roles in facilitating communication interception and service suspension requests from LEAs. Telia also explicitly notes its inability to interpret data gathered by intelligence services via signals intelligence.[15]

In summary, the transparency reports reveal considerable variation in how companies categorize and disclose data in response to LEA requests, highlighting inconsistencies in legal frameworks, data retention practices, and the influence of national security laws.

[10]Ruohonen, Jukka. (2023). Recent Trends in Cross-Border Data Access by Law Enforcement Agencies. 10.48550/arXiv.2302.09942.

[11] Ibid

[12] Ibid

[13] Ruohonen, Jukka. (2023). Recent Trends in Cross-Border Data Access by Law Enforcement Agencies. 10.48550/arXiv.2302.09942.

[14] Ibid

[15] Ruohonen, Jukka. (2023). Recent Trends in Cross-Border Data Access by Law Enforcement Agencies. 10.48550/arXiv.2302.09942.

5. CHALLENGES IN ACCESSING DATA THROUGH MLAT AND LR

According to European Commission's, more than 8 out of 10 criminal investigations needs electronic evidence and 66% of the case needs information from online service providers having servers outside the territorial limits of EU. Such data is not available for India but transparency report by Google received 25,275 user information request and 88,199 account requests from India in between July2021- December 2021, which is more than 250% increase from July 2019-December 2019, which is 10891 user requests and 25864 account requests.[16] Similar trend is also seen in Meta and Twitter transparency report.[17] Percentage increase is similar in United States. These figures provide a glimpse of the increasing need for electronic evidence in criminal investigations.

Once we look into the disclosures made by the online service providers, we get an understanding that India has been less successful in receiving data for enforcement. Figures 1 and 2 provide the comparative study of disclosures received by India and United States. Figure 3 also provides the data from Microsoft Transparency Report in relation to criminal law enforcement states very less data disclosures and the reasons for rejection of data disclosures. In 60% of the cases law enforcement requests were rejected by Microsoft due to lacking legal requirements i.e. a legal warrant or a subpoena.[18]

Figure1- US

Reporting period	Requests for disclosure of user information	Accounts	% of requests where some data produced
Jul2021-Dec2021	46.828	107.915	84%
Subpoenas	18.037	43.299	83%
Search warrants	23.924	49.572	85%
Other court orders	2.284	9.651	83%
Emergency disclosure requests	2.046	3.11	71%
Pen register orders	534	2.28	82%
Wiretap orders	3	3	33%
Preservation requests	16.032	49.71	

Figure 2 India Data Disclosure

Reporting period	Requests for disclosure of user information	Accounts	% of requests where some data produced
Jul2021-Dec2021	25,275	88,199	62%
Other legal requests	25,158	87,996	62%
Emergency disclosure requests	117	203	55%
Preservation requests	46	200	0

	Total Number of Law Enforcement Requests	Accounts / Users Specified in Requests	Law Enforcement Requests Resulting in Disclosure of Content	Law Enforcement Requests Resulting in Disclosure of Only Subscriber/Transactional (Non-Content) Data	Law Enforcement Requests Resulting in Disclosure of No Customer Data (No Data Found)	Law Enforcement Requests Resulting in Disclosure of No Customer Data (Request Rejected for Not Meeting Legal Requirements)
India	610	544	0.00%	29.02%	11.80%	59.18%

[16] "Google Transparency Report" (Google Transparency Report) <https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts;authority:IN;time:&lu=legal_process_breakdown&legal_process_breakdown=expanded:0,4> accessed January 9, 2023

[17] "Regulatory and Other Transparency Reports | Transparency Center" (Regulatory and Other Transparency Reports | Transparency Center) <https://transparency.fb.com/data/regulatory-transparency-reports/> accessed January 9, 2023; "Information Requests - Twitter Transparency Center" (Information Requests - Twitter Transparency Center) <https://transparency.twitter.com/en/reports/information-requests.html> accessed January 9, 2023

[18] "Law Enforcement Request Report | Microsoft CSR" (Microsoft) <https://www.microsoft.com/en-us/corporate-responsibility/lerr> accessed January 9, 2023

United Kingdom	3,148	3,929	0.00%	76.27%	15.31%	8.42%
United States	5,560	17,337	9.89%	43.78%	33.67%	12.66%

Figure 3- Microsoft Transparent report- 2021-22

6. CHALLENGES AND WAY FORWARD

India has shifted from a stringent data localisation approach, benefiting from expanding global digital trade and aligning more closely with international perspectives on the advantages of global digital commerce. However, ongoing discussions and debates about data privacy and localisation highlight that while regulations have made significant strides, practical implementation remains the key challenge. The recent revisions to the DPDP Bill 2019 and the newly enact Data Protection Act 2023 underscore the importance of collaboration and consensus-building in enacting these changes.[19]

Businesses face challenges in understanding their obligations under the new regulations and have called for greater clarity. The enforcement system, with its complex appellate process, has been viewed as impractical for many companies. While Europe's enforcement mechanisms predominantly target digital firms, India's law affects a wider range of industries. The Indian law, reflecting GDPR principles, extends comprehensive coverage and requires a legal foundation for data processing. It includes provisions on the processing of publicly accessible personal data, which could impact datasets used for generative AI training. However, significant flaws remain, such as allowing sectoral regulators to create their own rules without mandatory consultation with the Data Protection Board (DPB), which weakens uniformity in sector-specific regulations. India's approach to cross-border data transfers diverges significantly from models like the GDPR, prioritising law enforcement access to data over protecting individual rights, which has been viewed as detrimental to global standards. The complexity of the regulation raises compliance challenges, especially as global data protection standards become more intricate.[20]

Indian law enforcement faces challenges in building capacity and training. There is a need for future regulatory updates to better support data requests across borders and provide flexible data transfer mechanisms, such as certifications and trust marks, to ensure interoperability with global trading partners. The new data protection law addresses some of these challenges but may require bilateral treaties or international agreements on data governance. The legal frameworks of countries like Indonesia and Australia highlight the importance of having a coherent and consistent structure to regulate cross-border data transfers and the need for clear regulations to ensure certainty for businesses and promote responsible data management. Establishing best practices based on international standards is crucial, and India may consider adopting elements of the UK's model, which has demonstrated transparency in assessments related to data governance.

A more detailed discussion on law enforcement and government access to data in India is necessary, particularly in coordinating with international partners. Improvements are needed in the Mutual Legal Assistance (MLA) system, including digitisation and updates, to meet legitimate data requirements and reduce reliance on data localisation. India's data access and law enforcement system faces challenges, with frequent requests lacking legal justification and subject to political influence. Unlike other G7+ nations, India's data access authorities lack judicial oversight and have limited influence over cross-border data transfer rules, particularly in the Global South. While some data control measures have led to the creation of a negative list, it is crucial to establish and enforce standards that foster international relationships. Clarity is also needed regarding the authority of the DPB and the transparency of the rulemaking process. India's data governance framework faces significant challenges that hinder its aspirations for global leadership. To overcome these obstacles, collaborative efforts are required to improve inter-jurisdictional relations, especially in data transfer, access, and projects like the Cloud Act. These changes may not come swiftly, but they are essential for India's role in the global data governance landscape.

[19] Shekar K., & Sharma, V. (2023). Event Report | Roundtable on Influence of India's Digital Personal Data Protection Act 2023 on Cross-border Data Transfers: A Global Perspective. The Dialogue

[20] Ibid