IE University IE International Policy Review (IPR)
Journal **7 Issue 1** (2026)
https://ipr.blogs.ie.edu/

Streamlining Transatlantic Digital Evidence Sharing: Comparing the U.S.' Mutual Legal Assistance Treaty (MLAT) and the EU's European Investigation Order (EIO) in Drug Trafficking and Organized Crime Cases

Rebeca Boullosa Ordóñez

IE University, Segovia, Spain.
Business Administration & Bachelor of Laws.

E-mail: rboullosa.ieu2025@student.ie.edu

Published January 2026

Editor: Henry Johnson, Georgetown University

Abstract

This paper compares the US-EU Mutual Legal Assistance Treaty (MLAT) and the EU's European Investigation Order (EIO) in handling the process of sharing digital evidence for transnational drug-trafficking and organized-crime cases across borders. While both aim to make cooperation easier, the MLAT remains slow and centralized whereas the EIO is faster but stops at the EU borders. This study examines emerging tools—the CLOUD Act, the EU e-Evidence Regulation, and the Second Budapest Protocol—and argues for reforms that facilitate cooperation but balances efficiency with data protection, due process and judicial oversight in digital-evidence sharing.

Keywords: digital evidence, Mutual Legal Assistance Treaty, European Investigation Order

1. Introduction & Context

The rise of transnational drug-trafficking and organized crime networks has increased the need for digital evidence sharing across borders. Presently, authorities in one jurisdiction often need access to evidence stored in another jurisdiction, which creates a huge obstacle for investigators. Mainly, there are two principal frameworks in place to deal with this issue. In the U.S., the Mutual Legal Assistance Treaty System (MLAT) and in the EU, the European Investigation Order (EIO). As stated by the European Parliament, criminals have been increasingly relying on encrypted communication and social media platforms that are often outside of the investigating authorities reach. The need to gain cross-border access to data like emails and chats is more important now than ever before. It is not only about mere access, but also gaining it efficiently. For

example, the European Commission warned that current systems "often take up to ten months to process a request for data."[1] For fast moving crimes—such as organized and drug-related crimes—the data may be vital at that time, as delays can mean losing key leads or proof. However, the urgency of criminal cases must not come at the expense of fundamental rights protections, including privacy, due process and fair trial guarantees. Despite similar aims, the U.S. MLAT and EU EIO clash, impeding the seamless transfer of digital evidence. This essay argues that both frameworks require critical reforms such as creating conflict-of-law rules or joint deadlines across borders to ensure a more streamlined process to share digital evidence between the EU and U.S.

2. The U.S. Mutual Legal Assistance Treaty (MLAT) and The European Investigation Order (EIO)

In the U.S., MLAT is a formal agreement between governments to share evidence across borders. The U.S. Department of Justice (DOJ) explains that MLAT requests are executed under U.S law and are "transmitted between central authorities designated by each state."[2] In the case of requests from European countries, they first must go through the DOJ's Office of International Affairs (OIA) which would then decide if they meet the treaty's requirements. However, the MLAT framework is critically hindered by lengthy approval times, averaging 10 months for the request to be approved.[3] By then, the evidence may be irrelevant, as delays can make the evidence obsolete or unusable for prosecution. Each MLAT request requires multiple procedural steps, varying on the partner country's domestic laws. This process leaves little room for flexibility, especially in time-sensitive cases where the need for rapid evidence access can conflict with bureaucratic procedures. While the U.S. MLAT system reflects a state-centered approach to international cooperation, the EIO represents the EU's effort to simplify cross-border evidence sharing through mutual recognition and cooperation across EU borders. According to Article 9 of the Directive 2014/41/EU, an EIO must be "recognised and executed in the same way and under the same conditions as if the measure had been ordered by the executing State itself."[4] The EIO also lays out a specific standard form, requiring conforming to necessary and proportionate reasoning[5] and clear deadlines such as "authority shall take action within 30 days[...] and complete it within 90 days."[6] Furthermore,

[1] European Parliament Research Service, Electronic Evidence in Criminal Matters (Briefing, 2021) https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf accessed 24 November 2025; European Commission, 'Questions and Answers: Mandate for the EU–US cooperation on access to electronic evidence' (MEMO/19/863, 5 February 2019)

[2] United States Department of Justice, *'Criminal Division – Office of International Affairs: Frequently Asked Questions Regarding Mutual Legal Assistance in Criminal Matters'* (2022) https://www.justice.gov/criminal/criminal-oia/file/1498811/dl accessed 24 November 2025.

[3] European Commission, *'Questions and Answers: Mandate for the EU–US cooperation on access to electronic evidence'*(MEMO/19/863, 5 February 2019) https://ec.europa.eu/commission/presscorner/detail/en/memo_19_863 accessed 24 November 2025.

[4] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L130/1, art 9.

[5] ibid art 6.

[6] ibid art 12

the EIO only truly simplifies the process of evidence sharing when it is within the EU borders. When it comes to U.S. digital evidence sharing, the EIO is very time consuming and not efficient. This flaw largely stems from conflicting legal standards on data privacy, lawful access, and the absence of a direct channel between EU authorities and U.S. service providers. The growing use of encrypted platforms and digital technologies by criminals creates a pressing need to streamline cross-border evidence-sharing to prevent further crime.

2.1 Comparative Analysis of MLAT and EIO

While the MLAT and EU function on opposite sides of the world, they share many similarities. Specifically, they can be compared side by side through these four features: communication, efficiency, scope and privacy rules. In terms of communication, the MLAT is approved by central authorities of each state, while the EIO requests are directly transmitted "between competent judicial authorities."[7] Concerning efficiency, both the MLAT and EIO are relatively slow. The MLAT has an average response time of ten months while the EIO has a response time of 30-90 days.[8] Furthermore, when it comes to the scopes of both frameworks, they differ significantly. The MLAT, though global in scope, has numerous formalities that delay the process. On the other hand, the EIO is fast, but only inside the EU borders. Lastly, the privacy rules regarding both frameworks relate to the federal/national law of the nations. The MLAT's privacy rules depend on U.S. domestic law and treaty conditions, whereas the EIO privacy regulations are built in directly to EU law under fundamental rights and data protection standards already established.

3. Emerging Mechanisms for Digital Evidence Sharing

Alongside the MLAT and EIO, there have been other acts and regulations arising to begin the process of streamlining both frameworks. These policies include the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act, EU e-Evidence Regulation, and the Second Budapest Protocol. In the US, the CLOUD Act allows the U.S. to sign executive agreements allowing direct data requests between partner governments and U.S. tech companies.[9] However, this act only applies to partners of the U.S. for privacy reasons. Similar to the EIO, the act is efficient but quickly stops at the borders of the U.S. and their partner governments. In the EU, the e-Evidence Regulation allows EU prosecutors to send direct production orders to service providers in other EU states with a deadline in place of "ten days, or within eight hours in emergencies."[10] The

[7] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L130/1, art 7

[8] European Commission, *'Questions and Answers: Mandate for the EU–US cooperation on access to electronic evidence'*(MEMO/19/863, 5 February 2019) https://ec.europa.eu/commission/presscorner/detail/en/memo_19_863 accessed 24 November 2025 Directive 2014/41/EU (n 2) art 12.

[9] Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub L No 115-141, div V, 132 Stat 348 (2018) §105(d).

[10] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, [2023] OJ L189/1, art 10.

process of eliminating legal formalities for approval makes this process much more efficient than MLAT and similar policies. Still, the e-Evidence Regulation falls short of addressing key flaws of cross-border data sharing beyond the EU, especially with the U.S. Both the e-Evidence Regulation and the CLOUD Act shed light on a broader problem: each system improves efficiency domestically but struggles to bridge legal and procedural divides internationally. In response to these gaps, the Second Budapest Protocol aims to establish direct cooperation with service providers and faster data preservation. This allows for cross-border access to digital evidence under clearer rules and privacy protections.[11]

4. Points of Friction Between U.S. and EU Approaches

Before analyzing the ways in which both frameworks work, it is important to recognize the points that do not align between EU and U.S. policies. To begin, the provider obligations are a point of friction between both nations. U.S. providers are legally prohibited from sharing data directly to foreign authorities unless it is through a MLAT or CLOUD act request.[12] The wait times for legal approval can heavily strain the sharing process of crucial data. Moving on, secrecy and confidentiality across borders becomes a frequent point of friction between the EU and U.S. While the MLAT process gives no notice to data subjects when sharing information, the EIO allows confidentiality "where necessary to ensure the success of the investigation."[13] Furthermore, territoriality and data localisation is another point of friction between the nations' policies. Under U.S. federal law, data under the control of a U.S. provider is subject to U.S. jurisdiction, not the law where the data is being stored physically. However, EU states push for data to be stored locally in order to preserve privacy and control, which quickly complicates the process. As for human rights checks, the EIO and MLAT differ greatly. Executive review for MLAT requests and limited transparency contrast with judicial scrutiny and proportionality testing for EIO requests. The disparity between the two processes causes distrust between authorities on opposite sides of the Atlantic Ocean.[14]

4. Policy Reform and Future Cooperation

4.1 Problem Diagnosis: Why Current Systems Fail

While there are a lot of discrepancies between the EIO and MLAT, the fundamental problem lies between efficiency and fundamental rights and protections. The

[11] Council of Europe, *'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence'* (opened for signature 12 May 2022) CETS No 224 https://www.coe.int/en/web/cybercrime accessed 24 November 2025.

[12] Council of Europe, *'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence'* (opened for signature 12 May 2022) CETS No 224 https://www.coe.int/en/web/cybercrime accessed 24 November 2025.

[13] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L130/1, art 19.

[14] Kenneth Propp and others, *'Navigating Toward an EU–US Agreement on Electronic Evidence' Lawfare* (22 March 2023) https://www.lawfaremedia.org/article/navigating-toward-an-eu-u.s.-agreement-on-electronic-evidence accessed 24 November 2025.

MLAT's executive review, conducted by the DOJ's office, prioritizes treaty requirements but lacks the judicial review that EU states expect. This governmental approach checks requests for legal formality rather than necessity in relation to privacy rights protected under the EU Charter of Fundamental Rights. On the contrary, the EIO's judicial validation ensures independent courts review each request against those standards. This protects privacy, data protection, and due process rights. While this process provides more administrative checks, it contributes to the delays that harm urgent investigations. Overall, these frameworks lead to transatlantic mistrust: EU officials see executive review as not enough protection against rights, while U.S. officials perceive judicial validation as bureaucratic obstruction that allows for evidence destruction.

4.2 Reform Proposals with Implementation Details

Under existing policies such as the CLOUD Act, it is recommended to create joint deadlines for transatlantic exchanges and to build specific US-EU agreements that allow investigators to bypass formalities to speed up the process. However, these reforms must come from a hybrid oversight model functioning in two parts: for pressing requests involving threats, expedited executive review would authorize provisional access within 72 hours, while also allowing automatic judicial review within 7 days, to assess necessity and proportionality. If courts find that requests don't meet fundamental rights standards, evidence becomes inadmissible.

Providers between the EU and U.S. also tend to be caught in the middle of demands; the implementation of conflict-of-laws rules would ease the strain on providers by establishing remedies to where laws conflict or to clarify to which jurisdiction the data is subject.

In order to create a common template for requests, the EU-US should create a standardized procedure for approval forms. The Transatlantic Digital Evidence Request Form requires: identification of specific criminal acts, demonstration that evidence is directly relevant and cannot be obtained less intrusively, requesting data categories with justification, certification of compliance with both U.S. constitutional standards and EU Charter rights, and commitment to purpose limitation, with data subject notification within 90 days. Using secure electronic systems like e-CODEX could be especially useful to send requests safely through an Transatlantic Evidence Exchange Portal that automates compliance checks, tracks timelines, and maintains transparency.

4.3 How Reforms Address the Executive/Judicial Review Tension

The hybrid model recognizes that both review systems have their own pros and cons. Executive review enables necessary speed while judicial review provides rigorous rights protection. Rather than choosing between efficiency and rights, this two-tier system allows for both. Executive review handles initial authorization when time is pressing, but judicial review serves as an obligatory backstop catching violations and expressing accountability through retrospective but consequential oversight.

Acknowledgements

I would like to express my deepest gratitude to the IE International Policy Review for the opportunity to publish this work, and my editor, Henry Johnson for their guidance and mentorship throughout the process.

Bibliography

Primary Sources

Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub L No 115-141, div V, 132 Stat 348 (2018).

Council of Europe, 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence' (opened for signature 12 May 2022) CETS No 224 https://www.coe.int/en/web/cybercrime accessed 24 November 2025.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L130/1.

European Union and United States of America, Agreement on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences [2016] OJ L336/3.

Secondary Sources

European Commission, 'Questions and Answers: Mandate for the EU–US cooperation on access to electronic evidence' (MEMO/19/863, 5 February 2019) https://ec.europa.eu/commission/presscorner/detail/en/memo_19_863 accessed 24 November 2025.

European Commission, 'E-evidence – Cross-border access to electronic evidence' (2023) https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en accessed 24 November 2025.

European Commission, 'Report from the Commission to the European Parliament and the Council on the implementation of Directive 2014/41/EU regarding the European Investigation Order in criminal matters'COM (2021) 409 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0409accessed 24 November 2025.

European Parliament Research Service, Electronic Evidence in Criminal Matters (Briefing, 2021) https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf accessed 24 November 2025.

Fair Trials, 'The Achilles' Heel of the EU e-Evidence Regulation (EU) 2023/1543' (2023) https://www.fairtrials.org/articles/legal-analysis/the-achilles-heel-of-e-evidence-regulation-eu-2023-1543accessed 24 November 2025.

Kenneth Propp and others, 'Navigating Toward an EU–US Agreement on Electronic Evidence' *Lawfare* (22 March 2023) https://www.lawfaremedia.org/article/navigating-toward-an-eu-u.s.-agreement-on-electronic-evidence accessed 24 November 2025.

United States Department of Justice, 'Criminal Division – Office of International Affairs: Frequently Asked Questions Regarding Mutual Legal Assistance in Criminal Matters' (2022) https://www.justice.gov/criminal/criminal-oia/file/1498811/dl accessed 24 November 2025.

United States Department of Justice, 'Mutual Legal Assistance Treaties of the United States' (2022) https://www.justice.gov/criminal/criminal-oia/file/1498806/dl accessed 24 November 2025.