MARCH 2023

The CLOUD Act and Transatlantic Trust

By Georgia Wood and James A. Lewis

The United States and European Union are at a transitional moment in their transatlantic digital relationship. This transition affects the future of the **Clarifying Lawful Overseas Use of Data (CLOUD) Act**, a piece of U.S. legislation that aims to provide timely access to electronic evidence (e-evidence). Despite past disputes over data privacy and surveillance, both sides have found common ground—through the EU-U.S. Data Privacy Framework and the Organization for Economic Cooperation and Development (OECD)'s **Declaration on Government Access to Personal Data held by Private Sector Entities**—and created a forum for cooperation in digital trade through the Trade and Technology Council (TTC). Getting to this point, however, involved a complicated process, and despite real progress, the story is not yet over.

The United States and the European Union are each other's **top trading partners**. The transatlantic and data transfer relationship creates a **$7.1 trillion economic relationship**, so this is not a minor problem. All sides want to find solutions that permit digital trade to continue and that streamline the evidentiary process needed for law enforcement in the digital age.

This white paper looks at the tensions between the desire for timely law enforcement access to evidence, European concerns over digital sovereignty, and the mutual desire for a strengthened transatlantic relationship. The nature of cloud services means that data is often stored on one or several servers outside of a user's borders as well as outside of the country where a company's headquarters may be located. This makes economic sense but raises legal questions when governments wish to access electronic evidence that is stored outside of their jurisdiction for an investigation.

Genesis of the CLOUD Act

This is not a new problem, and enforcement agencies in many countries have complained for years about the slowness of conventional processes, such as Mutual Legal Assistance Treaties when compared to the transitory nature of digital evidence. A 2013 internal government **review** on the United States' ability to fulfill these requests noted it took approximately 10 months, with some requests taking much longer.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Conflict over government access to data in another jurisdiction came to a head in the 2013 **Microsoft Ireland** case. In 2013, the United States presented Microsoft with a warrant to disclose data—which the company found to be stored in a data center in Dublin. Given the data's location, Microsoft argued that a U.S. court did not have the authority to issue a warrant for data stored abroad and asked the court to suppress the order. While the reasoning of the U.S. District Court for the Southern District of New York that material control over the data—regardless of where stored—was enough for Microsoft to comply with the order, the U.S. Court of Appeals for the Second Circuit found this to be an unauthorized extraterritorial application of U.S. law.

The United States appealed the Second Circuit's decision to the Supreme Court, **referencing** other courts had previously found requiring U.S. companies to comply with Stored Communications Act (SCA) warrants outside of the United States is a domestic application of the law. Before the Supreme Court ruled, Congress passed the CLOUD Act and made the Microsoft Ireland case moot. The CLOUD Act amended the SCA to clarify that communication service providers must comply with legal requests for data from the U.S. government, "regardless of whether such communication, record, or other information is located within or outside of the United States."

While the CLOUD Act confirmed the legality of U.S. government requests for data stored by U.S. communications service providers outside of the United States, it also created concerns in the European Union over extraterritorial application of U.S. law. Building on the mistrust over user privacy and data protection that was exacerbated in part by the Snowden revelations about surveillance, the CLOUD Act faced criticism and **concern** from EU officials worried that it would infringe upon European digital sovereignty. Digital sovereignty, or the control of technology operating under one's jurisdiction, is a **key goal** for EU member states.

Intent of CLOUD Act Agreements

Service providers have traditionally been hesitant to answer foreign government requests for data because of fears that they could be found in violation of domestic laws governing privacy and data protection. The CLOUD Act was intended to address this, however, with a second provision that allowed the U.S. government to enter into executive agreements with third countries for reciprocal expedited access to e-evidence held by providers based abroad. This provision was frequently misunderstood.

The bilateral agreements contemplated under the CLOUD Act were intended to remove these conflicts when both the requesting and supplying jurisdictions share similar privacy and civil liberties protections. An agreement under the **CLOUD Act** requires an assessment of the foreign country's domestic law to ensure it respects "substantive and procedural protections for privacy and civil liberties" and limits who can be targeted. Any orders issued under the CLOUD Act must "be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism" and must be subject to review or oversight by a judicial authority. This provision of the CLOUD Act was intended to create a quicker and more efficient way for law enforcement agencies to gain access to electronic data held outside of their borders by global cloud service providers. The act does not replace the Mutual Legal Assistance Treaty process, but rather provides an additional method of cross-border data access.

Despite a shared transatlantic recognition of the problem, the United States has only been able to reach CLOUD Act agreements with the United Kingdom and Australia and is reportedly negotiating with Canada. This slow pace means that the environment for CLOUD Act negotiations is being reshaped by transatlantic developments and new agreements on data and privacy.

> *This slow pace means that the environment for CLOUD Act negotiations is being reshaped by transatlantic developments and new agreements on data and privacy.*

In September 2019, a joint U.S.-EU **statement** announced the beginning of formal negotiations on an agreement for facilitating access to e-evidence in criminal investigations. This negotiation was supposed to happen in parallel with the European Union's own framework for e-evidence—the E-Evidence Regulation. Initially, internal EU disagreements prevented the regulation from being enacted and the negotiations with the United States from proceeding. However, in January 2023, the European Council and European Parliament reached **agreement** on the draft regulation and the draft directive on cross-border access to e-evidence with similar authorities as the CLOUD Act. This signals real progress on reaching an e-evidence agreement between the European Union and the United States and the Department of Justice **announced** in March 2023 that negotiations had resumed with the European Union.

Conflicts between EU Law and the CLOUD Act

Without a U.S.-EU agreement on access to e-evidence, conflicts between the CLOUD Act and EU regulation remain. An initial **assessment** commissioned by European authorities of the compatibility between the CLOUD Act and EU legal framework identified the main potential conflict to be Article 48 of the General Data Protection Regulation (GDPR) on transfers or disclosures not authorized by EU law. Article 48 outlines that a foreign court order would not be sufficient to make a transfer lawful unless "based on an international agreement." The European Commission's objectives for an international agreement **include** enhancing the legal certainty between the jurisdictions and allowing for the transfer of e-evidence on a reciprocal basis while ensuring respect for EU law. The European Commission **argued** in the Microsoft Ireland case (through an external brief) that Article 48 "makes clear that a foreign court order does not, as such, make a transfer lawful under the GDPR."

Article 49 of the GDPR establishes the conditions under which an international transfer could occur if an international agreement is not in place. Specifically, the first paragraph of the article stipulates, among other potential conditions, that the subject is notified and provided consent, or the transfer is necessary for "important reasons of public interest." A CLOUD Act transfer could also be considered lawful under Article 6(1)(d) when the transfer is in the vital interest of data subjects themselves (e.g., accessing personal data concerning abducted minors). The EU assessment concluded that an "international agreement containing strong procedural and substantive fundamental rights safeguards appears the most appropriate instrument to ensure the necessary level of protection for EU data subjects and legal certainty for businesses."

Progress on a CLOUD Act agreement between the United States and the European Union was complicated by decisions made by the Court of Justice of the European Union (CJEU). Since the 2013

Snowden revelations that exposed mass surveillance by the U.S. National Security Agency (NSA) for counterterrorism purposes, there has been increased concern in Europe over U.S. government access to data concerning EU citizens. In 2015, the CJEU invalidated the 2000 Safe Harbor Privacy Principles agreement between the United States and the European Union in a decision known as **Schrems I**—the name coming from Austrian privacy activist Max Schrems, who has launched several complaints to European data protection agencies over Facebook's handling of user data. In the Schrems I decision, the CJEU cited the Snowden revelations as demonstrating "a 'significant overreach' on the part of the NSA and other federal agencies" and that data transfers to the United States could violate Article 7—respect for private and family life—of the **Charter of Fundamental Rights of the European Union**.

After Schrems I, work to rebuild the legal basis for transatlantic data flows began. This resulted in the adequacy **decision** of the Privacy Shield framework, a renewed agreement between the United States and the European Union on privacy principles. However, in 2020, the CJEU invalidated Privacy Shield in a decision known as Schrems II, in which the European Union was principally concerned with U.S. regulations enabling certain signals intelligence activities. The decision referenced Section 702 of the U.S. Foreign Intelligence Surveillance Act, which allows the U.S. government to **compel communication service providers** to assist in the surveillance of foreign persons outside the country, and U.S. Executive Order 12333, which denotes when intelligence agencies can **engage in foreign intelligence surveillance abroad**. Schrems II **outlined** two necessary benchmarks for the transatlantic data flows to be in compliance with EU law: U.S. surveillance activities should be limited to what is necessary and proportional and should be subject to judicial redress.

In March 2022, the United States and European Union **agreed** in principle to the EU-U.S. Data Privacy Framework to address concerns raised in Schrems II. This framework was then implemented by the October 2022 U.S. "**Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities"** (EO 14086). EO 14086 **pledges** to "tailor U.S. signals intelligence collection to what is 'necessary' and 'proportionate' to protect both national interests and individual privacy and civil liberties" and enables a redress mechanism through the establishment of the Data Protection Review Court. In response, the European Union issued a draft adequacy **decision,** and it is expected that the legal framework for transatlantic data flows will be reinstated. The renewed framework highlights the common ground the United States and European Union have on access to data.

European Response

Concerns with the CLOUD Act and the application of non-European laws to European jurisdictions sparked a flurry of action in Europe. Developed in 2020, the **European strategy for data** is an initiative to ensure European competitiveness and data sovereignty amid concerns over extraterritorial laws in the transfer of data. The strategy explicitly states that the application of the CLOUD Act is a risk to the data of EU citizens and businesses stored by cloud service providers and subject to third-country legislation. The strategy led to the creation of the **Data Governance Act** (DGA) and **Data Act**. While the GDPR provides a governance framework for personal data, the DGA and the proposed Data Act provide an additional framework for the reuse, transfer, and protection of nonpersonal data. Personal data is information relating to identifiable individuals, whereas nonpersonal data is information not related to an identifiable person.

Both acts aim to ensure that Europe benefits from the data it creates. The DGA looks to make more data available, combat technical barriers in data reuse, and advance trust in data sharing across the European Union. The Data Act tackles the question of who can create value from European data and where this can take place. In the DGA, international access and transfer of EU data is limited—compliance with a third-country decision that compels the disclosure of data held in the European Union must be based on an international agreement between the third country and the European Union or a member state. In the absence of an international agreement, Article 31 outlines that foreign access requests are honored only when they are deemed proportional and specific, subject to third-party court or tribunal review, and considerate of EU and member state legal interests.

The proposal for the Data Act contains similar provisions—if no international agreement exists, the transfer "should only be allowed if it has been verified that the third country's legal system requires the reasons and proportionality of the decision to be set out, that the court order or the decision is specific in character, and that the reasoned objection of the addressee is subject to a review by a competent court in the third country, which is empowered to take duly into account the relevant legal interests of the provider of such data"—and its recent revisions **reportedly** align language concerning international data transfers more closely with the DGA. These rules will **complicate** international transfers of nonpersonal data, as each request must undergo a review process by "competent authorities" designated by the member states to ensure that adequate safeguards for compliance with the DGA—and the Data Act once enacted—are in place. Potential conflicts between the CLOUD Act and the GDPR remain, and new legislation, such as the DGA and the Data Act, will further complicate the legal basis for nonpersonal data transfers.

SECURITY STANDARDS FOR CLOUD SERVICE PROVIDERS

European action is also focused on regulating cloud service providers with security requirements that include sovereignty provisions, and, in the case of France, forced technology transfer to local joint venture partners as a condition of market entry.

In May 2021, the **French National Cloud Strategy** outlined the development of a "Cloud de confiance" label to further protect French data while enabling the use of innovative services. This label is based on the certification scheme SecNumCloud—a security standard for cloud service providers **launched** in 2016. The strategy outlined that the Cloud de confiance label would allow the creation of new cloud service companies with European ownership and foreign technology to ensure that cloud service providers operating in France provide both legal and technical protection.

France **updated** the sovereignty requirements in SecNumCloud in March 2022 following the strategy's direction to focus on integrating protection criteria with respect to extra-European law. The provisions include joint ownership requirements to preclude majority foreign-owned providers from being SecNumCloud certified. Joint-ownership requirements similar to those used by China sparked a number of partnerships between French and U.S. companies to build joint cloud services with majority French ownership, such as between **Google Cloud and Thales** and between **Capgemini, Orange, and Microsoft**.

SecNumCloud contains provisions that go beyond cybersecurity requirements. Its considerations of foreign jurisdiction and control of data relate more to sovereignty than to cybersecurity. The updated SecNumCloud certification includes requirements for the "central administration or

main establishment of the service provider" to be located in the European Union and localization requirements that the provider must store and process customer and technical data in the European Union. The SecNumCloud requirements have met with opposition from **industry** since they could impact security and raise costs. There are also concerns overs its localization requirements and immunity to extraterritorial legislation. Some analysts **argue** that SecNumCloud requirements "breach both France and the European Union's (EU) commitments under the World Trade Organization's General Agreement on Trade in Services."

The European Union Agency for Cybersecurity (ENISA) is also developing its certification **scheme for cloud services** (EUCS), as directed by Article 48 of the European Union's **Cybersecurity Act**. The scheme is a cybersecurity certification system for cloud services with three assurance levels: basic, substantial, and high. The basic requirements are meant to define a minimum acceptable baseline for cloud cybersecurity; the substantial requirements are meant to define standards to mitigate against cyberattacks carried out by actors with limited skills and resources; and the high requirements are meant to define standards to mitigate against cyberattacks carried out by actors with significant skills and resources. In April 2022, the European Commission **reportedly** asked ENISA to include sovereignty requirements in the updated version of EUCS. The proposed sovereignty requirements would only apply to high level certifications. According to **reporting** on the draft requirements, the provider would have to be "headquartered in Europe, not be controlled by any non-EU entity," and be "completely independent from non-EU laws."

Although currently voluntary, the **Directive on Measures for a High Common Level of Cybersecurity across the Union** (NIS2 Directive), approved in November 2022, gives member states the ability to mandate compliance with EU certification standards, such as EUCS. The directive states that "in order to demonstrate compliance with certain requirements of Article 18, member states may require essential and important entities to certify certain ICT [information and communications technology] products, ICT services, and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881."

The drafting of EUCS has been criticized for a lack of transparency and accountability, and industry associations have raised concerns about the politization of the process in multiple **joint memos**. EUCS is also seen as problematic by European member states. Denmark, Estonia, Greece, Ireland, the Netherlands, Poland, and Sweden have raised **concerns** about the requirements. At the December 2022 TTC meeting, U.S. secretary of commerce Gina Raimondo offered the TTC as a potential avenue to present differing opinions over EUCS.

ENISA **will present** an updated draft of the requirements to the European Cybersecurity Certification Group (ECCG)—a coalition of cybersecurity authorities in member states—which will then issue an opinion for ENISA's consideration. The ECCG will then have three months to form a draft opinion, after which ENISA will have six months to present a final draft to the commission. EUCS is set to be implemented in 2025.

Skepticism about these EU initiatives is driven in part by the fact that the location of data does not ensure the security of data. Best practices, such as the use of encryption, are what make data secure, regardless of where it is located. Inadequately secured data is vulnerable wherever it is located. Given the importance of the transatlantic relationship, further progress to bridge legal differences between the United States and the European Union should remain a priority on both sides of the Atlantic.

> *Skepticism about these EU initiatives is driven in part by the fact that the location of data does not ensure the security of data. Best practices, such as the use of encryption, are what make data secure, regardless of where it is located.*

Concerns over European Action

Within the European Union, there have been **calls** to discuss sovereignty requirements in cybersecurity certification schemes at the European Council level, rather than ENISA, to ensure adequate input from member states. Countries noted the political nature of these sovereignty requirements and requested increased transparency and conversation on the EUCS drafting process. Germany suggested these EUCS requirements be discussed through the European Council's Horizontal Working Party on Cyber Issues or the Working Party on Telecommunications and Information Society. A recent **document** from member states explored alternative solutions to safeguard against the application of non-EU law in the context of EUCS, including more specific levels of assurances for critical uses and modifying pending EU legislation to discuss the issue at a political level.

Backlash from governments and industry is largely rooted in the potential damage from data localization requirements on innovation and security in the European Union. U.S. companies account for **72 percent** of the European cloud market, limiting Europe's industry choice through these requirements will raise costs and create a gaps in capacity for European industry. The **fate** of Gaia-X, an initiative launched in 2020 to defend European interests and values in the cloud, suggests that both sides would benefit from a cooperative solution.

Alternatives have been discussed to address European concerns about extraterritorial access to data. Companies in particular point to **encryption** over localization as the key protection for data. They have also accelerated partnerships with domestic providers to ensure local storage and compliance with country regulations. Google, for example, is specifically **expanding** their trusted partner cloud program to ensure collaboration with local providers.

Data localization could limit access to cybersecurity resources, hinder incident response efforts, and create obstacles to information sharing. One of the first things Ukraine had to do in the face of Russian cyberattacks in 2022 was **revoke** its data localization rules and migrate data to the extraterritorially located cloud. There is a growing sense in Washington that digital sovereignty and cybersecurity are used as an excuse for protectionism (exacerbated by **remarks** from some senior European officials calling for an exclusion of U.S. cloud providers), but this is a dispute that can be avoided.

Looking Ahead

Two principles that build on recent agreements can help guide transatlantic discussion to a mutually agreeable outcome:

1. Build on shared values established in the OECD declaration.

   Moving forward, the United States and European Union can build on the recent progress to build common understandings for sovereignty and for the requirements for streamlined access to digital evidence. There is an opportunity to build on the OECD's Declaration on Government Access to Personal Data held by Private Sector Entities (agreed on in December 2022 after two years of negotiations). These joint principles apply to government activities, and for the United States, this **includes** requests made under the CLOUD Act.

   The declaration marked the first intergovernmental agreement on "common approaches to safeguarding privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes" and emphasized the countries' "significant commonalities" on the topic. The principles include necessity, proportionality, transparency, oversight, and redress—areas that can be foundational in the creation of joint understandings between the United States and the European Union and a starting point for negotiations on a formal e-evidence agreement. These principles identify an emerging common language that can be built upon for a legally binding treaty.

2. Use the EU-U.S. Data Privacy Framework as a model for joint understandings.

   Recent progress on the EU-U.S. Data Privacy Framework also points to joint understandings that can be key for the negotiation of an e-evidence agreement—the draft adequacy **decision** references U.S. criminal legal processes as providing adequate safeguards for European data. Prior to the implementation of these sovereignty requirements in the European Union, conversation with the United States on how to reach common ground will be key to EU innovation and security.

   It is an open question as to whether pursuing CLOUD Act agreements with EU countries could be superseded by these agreements, and with the U.S.-EU discussion over data governance, there are encouraging signs. There are shared transatlantic concerns over crime and law enforcement which signal that agreement remains possible. The problem is not going away, and the outlines of a solution are visible. ■

Georgia Wood *is a program manager and research associate with the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***James A. Lewis*** *is senior vice president and director of the CSIS Strategic Technologies Program.*

This report is made possible by general support to CSIS.