The US CLOUD Act: Myths vs. Facts

April 2019

The U.S. CLOUD Act provides enhanced protections for individual privacy and clarifies the circumstances under which U.S. law enforcement may potentially access data, regardless of where it is stored, pursuant to specific legal processes and independent judicial oversight. Conversely,, the CLOUD Act also empowers the United States government to enter into new bilateral agreements, known as Executive Agreements, with other governments that would enable law enforcement agencies to access data across each other's borders to investigate and prosecute crimes, subject to an agreed-upon set of processes and controls negotiated between the two governments.

Certain misconceptions about the scope of the of the legislation, the types of service providers and data subject to the CLOUD Act, its extraterritorial effects, and the legal process restrictions have raised some questions about the impact on the privacy of citizens of the European Union (EU). This white paper seeks to address those common misconceptions by separating myths from the facts about the CLOUD Act.

X MYTH: The CLOUD Act will be used by US law enforcement to access data stored by US-based cloud providers.

✓ FACT: The CLOUD Act applies to several categories of service providers if they are subject to jurisdiction in the United States, regardless of where they are based. The US Department of Justice has adopted a policy of not seeking data from the service provider, however, unless seeking data from the enterprise customer would sacrifice the investigation.

- **The CLOUD Act applies to two types of technology providers:**
  (1) electronic communications services ("ECS providers") and
  (2) remote computing services ("RCS providers").

ECS providers are defined as services that provide users with "the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

RCS providers are defined as services that provide "to the public" "computer storage or processing services" using an electronic communications system. 18 U.S.C. § 2711(2).

In December 2017, the U.S. Department of Justice issued guidance limiting the circumstances in which federal prosecutors should serve legal requests on technology companies for enterprise customer data.[1] **Specifically, the U.S. Department of Justice guidance provides that prosecutors "should seek data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation[2]."** This guidance recognizes that in many cases, the enterprise customer—and not the cloud provider—will be the appropriate entity to respond to *legal process.*[3] Service providers typically do not have any detailed or practical insight into what data they handle on behalf of their enterprise customers, who are therefore in a much better position to respond to the demand as it relates to their *own* data.

Further, in April 2019, the U.S Department of Justice, released a white paper to further clarify CLOUD Act, but providing descriptions of the effect, scope, and implications of the Act, as well as answers to frequently asked questions[4].

- **Service providers are subject to the CLOUD Act if they are subject to jurisdiction in the United States, regardless of where they are based.**

Legal process issued under the CLOUD Act may reach data in the possession, custody, or control of an ECS or RCS provider that is *subject to jurisdiction* in the United States.

The exercise of personal jurisdiction by U.S. courts is limited by the Due Process Clause of the U.S. Constitution and is accordingly equivalent to a fundamental right in the EU. The CLOUD Act does not affect whether a company is subject to jurisdiction in the United States. Rather, *legal process* issued under the CLOUD Act may only be enforced against companies *already* subject to jurisdiction in the U.S.

A company does not need to be headquartered in the United States to be subject to U.S. jurisdiction. A company is subject, for example, if "minimum contacts" exist – i.e., when a business "purposefully avails" itself of the privilege of conducting business in the United States, such as by obtaining contracts with U.S.

---

[1] *See* Computer Crime and Intellectual Property Section, Criminal Division, U.S. Dep't of Justice, Seeking Enterprise Customer Data Held by Cloud Service Providers, December 2017, *available at* https://www.justice.gov/criminal-ccips/file/1017511/download .

[2] A similar provision is contained in the proposed E-evidence regulation in Article 5(6) available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN

[3] In U.S. law, a legal process is a formal court order, writ or warrant by which a court obtains jurisdiction over a person or property.

[4] "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act" https://www.justice.gov/opa/press-release/file/1153446/download

customers; the business would accordingly be subject to specific jurisdiction for suits related to those contacts.

The limited scope of personal jurisdiction in the U.S. suggests that the effective jurisdictional reach of the CLOUD Act is meaningfully narrower in key respects than will be the case in the EU when the E-Evidence Directive and E-Evidence Regulation are passed, since these EU measures will effectively make service providers subject to Member State Law Enforcement Accessorders if their service is accessible to a significant number of users in the EU. This accessibility standard is likely to be broader than the "minimum contacts" standard under U.S. law, which is further restricted by the notions of "fair play and substantial justice."

As a general matter, if a provider has the technical ability to access data, then that data would likely be found to be within its possession, custody, or control of the data for purposes of U.S. law. This is not limited to U.S. service providers. To the extent any provider subject to U.S. jurisdiction has the technical ability to access data, it would likely to be found to have possession, custody or control of that data.

While the test for determining if a provider is in possession, custody, or control is fact-specific and varies across U.S. jurisdictions, it is generally satisfied when a provider has *either*: (1) the legal right to access the information or (2) the practical ability to do so.

- **The CLOUD Act will apply to companies established outside the United States that also offer services in the United States. These companies can be required directly by US authorities regardless of the location of its hosting data.**

Indeed, such companies may have "minimum contacts" that support jurisdiction in the U.S. While the minimum contacts analysis is fact-specific and typically considers whether the entity purposefully directed its activities at the U.S. forum, the contacts need only be minimal. For example, minimum contacts may exist when a business purposefully seeking contracts with U.S. customers. An ECS or RCS provider that is subject to jurisdiction in the United States is obligated to comply with a CLOUD Act request regardless of where the data sought is hosted.

ECS and RCS providers are subject to the CLOUD Act regardless of whether they are considered "US persons" and irrespective of their capital structure (i.e. a European headquartered company whose capital is majority-owned by US funds). So long as an ECS or RCS provider has sufficient "minimum contacts" with the United States to support the exercise of jurisdiction in U.S. courts and has possession, custody, or control of the data sought, then it is subject to *legal process* issued under the CLOUD Act.

If a European subsidiary of a U.S. company had sufficient "minimum contacts" with the United States to support jurisdiction in U.S. courts, and has possession, custody, or control of the data sought, then it is subject to *legal process* issued under the CLOUD Act.

X MYTH: US law enforcement authorities will have unfettered access to the contents of stored communications.

✓ FACT: The initiating procedure for government access to communications content is a search warrant, signed by an independent U.S. judge.

Under the CLOUD Act and constitutional standards applicable to *legal process* issued under the CLOUD Act, U.S. authorities must obtain a warrant for the content of stored electronic communications, regardless of the age of those communications. *See*, *e.g.*, *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). To obtain such a warrant, a U.S. prosecutor must convince a court that probable cause exists that a specific crime has occurred or is occurring and that the place to be searched, such as an email account, contains evidence of that specific crime. This finding is made by an independent judicial authority.

Under the CLOUD Act[5], subpoenas may only be used to seek limited forms of basic subscriber information (such as name, address and billing information) and can under no circumstance be used to compel the disclosure of content.

Only a limited set of data is available without prior court approval and providers may challenge each of these forms of legal process when there is a potential for conflict with foreign law.

- Basic subscriber information is a limited set of identifying information (including a subscriber's name, address, billing information, and other specific forms of identifying information) that may be obtained by a subpoena, without prior court approval.
- Non-content information, including transactional data, requires a court order finding specific and articulable facts showing there are reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation.
- Content of stored communications is generally obtained by warrant, which requires a court to find probable cause to believe the account in question contains evidence of a crime.

The U.S. Department of Justice explained these legal process standards, requirements and restrictions to the EU Commission and other relevant EU authorities in a letter included in the package of EU-U.S. Privacy Shield materials provided to the EU Commission on July 7, 2016[6]. These standards were not changed or reduced by the CLOUD Act.

U.S. law enforcement must apply to a court -- i.e., an independent judicial authority -- for approval of either a warrant for content or court order for non-content information other than basic subscriber information before serving that warrant / order on an ECS or RCS provider. This application must make the showing required for the court to issue the warrant or court order. In fact, the CLOUD Act has introduced additional privacy and other safeguards and provides additional avenues to services providers to challenge these requests (see below).

[5] This document focuses solely data access requests done in the purpose of criminal investigations based on the CLOUD Act and not for data access requests that could be made for the purposes of national security under other US legislation, FISA for instance.

[6] https://www.federalregister.gov/documents/2016/08/02/2016-17961/privacy-shield-framework

For a *warrant to obtain content*, the showing must convince the court that probable cause exists to believe that a specific crime has occurred or is occurring and that the place to be searched, such as an email account, contains evidence of that specific crime. Providers who furnish the content of communications to a U.S. or foreign government, in the absence of such a search warrant, risk civil and criminal liability. For an *order to obtain non-content* (including transactional data), the showing must convince the court that there are specific and articulable facts showing there are reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation.

With regard to confidentiality of data access requests, ECS and RCS providers may notify their customers of requests made by US law enforcement authorities, unless a court issues an order specifically prohibiting such notice. Such an order may only issue in very specific and limited circumstances which are typically less ubiquitous in a corporate customer context -- specifically, if a court finds that notification to the customer will result in endangering the life or physical safety of an individual, flight from prosecution, destruction of or tampering with evidence, intimidation of potential witnesses, or otherwise seriously jeopardizing an investigation or unduly delaying a trial.

X MYTH: The CLOUD Act allows for data access requests to be made on various grounds, including civil, administrative or commercial inquiries

✓ FACT: Warrants obtained under the CLOUD Act can only be issued by U.S. courts in connection with the investigation of criminal activity

Warrants may only be issued by U.S. courts in connection with the investigation of criminal activity, although there is no requirement that warrants are only issued in connection with investigations of "serious crimes." Still, a warrant may only be issued when a U.S. prosecutor has convinced a court that probable cause exists that a specific crime has occurred or is occurring and that the place to be searched, such as an email account, contains evidence of that specific crime. This finding is made by an independent judicial authority and not by the law enforcement authority itself.

The investigation of *criminal activity* for which a warrant may be issued in connection includes specific economic and corruption offenses, such as fraud, money laundering, or similar offenses. The CLOUD Act, however, does not authorize the issuance of *legal process* in connection with economic espionage, because such a request would not be in connection with an investigation of criminal activity. As a result, if any CLOUD Act warrant were used to obtain commercially sensitive information of foreign corporations for the purpose of assisting U.S. companies, it would be contrary to U.S. law and may create criminal and civil liability for misuse for all parties involved.

Under the CLOUD Act and constitutional standards applicable to *legal process* issued under the CLOUD Act, U.S. authorities obtain a warrant for the content of stored electronic communications. A warrant may only issue if a court -- i.e., an independent judicial authority -- finds that probable cause exists that a specific crime has occurred or is occurring and that the place to be searched, such as an email account, contains evidence of that specific crime.

As warrants may only be issued in connection with criminal investigations. The disclosure of content pursuant to a warrant may therefore not be made in a civil, administrative, or commercial inquiry.

X MYTH: The CLOUD Act can create conflicts of laws and does not provide for means of recourse

✓ FACT: The CLOUD Act contains robust safeguards and, even in the absence of an Executive Agreement between the United States and a foreign country, it offers a common law recourse on comity

The CLOUD Act does not require an executive agreement to be in place between the U.S. and a foreign country for an ECS or RCS provider to be able to challenge *legal process* issued under the Act on grounds of international comity. Rather, the CLOUD Act expressly recognizes the ability of providers to challenge *legal process* issued under the CLOUD Act on grounds of international comity under longstanding common law principles.

Service providers can therefore seek to modify or quash *legal process* issued under the CLOUD Act by filing a motion with the Court. There are two mechanisms for doing so:

- First, providers may seek to set aside *legal process* issued under the CLOUD Act based on conflicts with a foreign country's law, when that country has not entered into an international agreement authorized by the Act. The CLOUD Act specifically preserves the ability of service providers to bring such common law "comity" challenges.[7] Indeed, the U.S. Department of Justice has recognized the availability of such challenges. In an argument before the Supreme Court, the Department of Justice said that when U.S. *legal process* conflicts with a foreign law "courts conduct a comity analysis."[8] Similarly, in a brief to the Supreme Court, the Department of Justice said that the "CLOUD Act does not affect the availability or application of a common-law comity analysis."[9]

- Second, and in cases when a country has entered into an international agreement authorized by the Act, the CLOUD Act creates a new statutory mechanism for providers to seek to set aside a warrant issued by a U.S. court if: (1) the subscriber is not a U.S. person and (2) the disclosure

[7] 18 U.S.C. 2703 note (2018) (Rule of Construction).
[8] Transcript of Oral Argument at 27, *United States v. Microsoft Corp*., No. 17-2 (2018), *available at* https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/17-2_j4ek.pdf.
[9] Brief of Petitioner at 5, *United States v. Microsoft Corp.*, No. 17-2 (2018), *available at* https://www.supremecourt.gov/DocketPDF/17/17-2/41851/20180330172237829_17-2motUnitedStates.pdf.

sought would create a material risk of violating the laws of a qualifying government that has entered into a bilateral agreement of the type contemplated by the Act. The Act sets out a list of factors a court should take into account in assessing such a challenge, including the interest of the foreign government in prohibiting disclosure, the U.S. government's interest in the information, the location and nationality of the subscriber, and the likelihood of timely and effective access to the information through other means.[10] This also ties in with the fact that the CLOUD Act is not designed to provide unfettered and indiscriminate access to data held by service providers, but to facilitate the investigation of criminal activity as it relates to US persons, while providing more legal certainty and additional safeguards for both service providers and their enterprise customers.

Moreover, when the European Commission concluded its second annual review on implementation of the Privacy Shield agreement in December 2018, nine months after the passage of the CLOUD Act, found no evidence that the CLOUD Act undermined protections or commitments set forth in the Privacy Shield agreement.

In fact, the Commission Staff Working Group supporting the review found that "the CLOUD Act subjects the conclusion of such executive agreements to a number of safeguards and requirements: the foreign domestic law and its implementation must provide sufficient substantive and procedural protections for privacy and civil liberties…orders must be limited to address serious crimes, comply with the foreign domestic law, be specifically targeted and be subject to independent review or oversight."[11]

[10] 18 U.S.C. 2703(h)(2).

[11] "Commission Staff Working Document Accompanying the Report from the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU-U.S. Privacy Shield," SWD (2018) 497, December 19, 2018. https://ec.europa.eu/info/sites/info/files/staff_working_document_-_second_annual_review.pdf.

X MYTH: The CLOUD Act is a one-way street, enabling the US to access EU citizens' data without reciprocal EU access to US data.

✓ FACT: The CLOUD Act explicitly provides for bilateral executive agreements and makes provision for non-U.S. authorities to access content stored by U.S. companies subject to appropriate restrictions and safeguards.

The CLOUD Act provides a framework to enable bilateral agreements between the US and other national governments to provide for mutual law enforcement access to data stored by service providers in the other country. Such agreements codify mutually binding rules and procedures for obtaining evidence in the interest of ensuring security while establishing non-negotiable safeguards for human rights that both sides must respect.

The practical aspects of executions of *legal processes* in the context of an Executive Agreement will depend on the content and provisions of the relevant Executive Agreement and the laws of the countries that sign such an agreement. No such agreements have taken effect yet.