Promoting Public Safety, Privacy, and the Rule of Law Around the World:

The Purpose and Impact of the CLOUD Act

White Paper

April 2019

www.justice.gov/CLOUDAct

Introduction

The United States enacted the CLOUD Act to speed access to electronic information held by U.S.-based global providers that is critical to our foreign partners' investigations of serious crime, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime. Our foreign partners have long expressed concerns that the mutual legal assistance process is too cumbersome to handle their growing needs for this type of electronic evidence in a timely manner. The assistance requests the United States receives often seek electronic information related to individuals or entities located in other countries, and the only connection of the investigation to the United States is that the evidence happens to be held by a U.S.-based global provider. The CLOUD Act is designed to permit our foreign partners that have robust protections for privacy and civil liberties to enter into executive agreements with the United States to obtain access to this electronic evidence, wherever it happens to be located, in order to fight serious crime and terrorism. The CLOUD Act thus represents a new paradigm: an efficient, privacy and civil liberties-protective approach to ensure effective access to electronic data that lies beyond a requesting country's reach due to the revolution in electronic communications, recent innovations in the way global technology companies configure their systems, and the legacy of 20th century legal frameworks. The CLOUD Act authorizes executive agreements between the United States and trusted foreign partners that will make both nations' citizens safer, while at the same time ensuring a high level of protection of those citizens' rights.

Background

Often electronic evidence is held by communications service providers ("CSPs") with global operations. They may have customers all over the world and company offices and data storage facilities located in many different countries. As a result, CSPs and the data they control may be subject to more than one country's laws. Conflicting legal obligations may arise when a CSP receives an order from one government requiring the disclosure of data, but another government restricts disclosure of that same data. These potential legal conflicts present significant challenges to governments' ability to acquire electronic evidence that may be vital to pursuing criminal investigations in a timely, efficient manner.

Many governments can rely on their domestic laws to require CSPs within their jurisdiction to disclose electronic data under the companies' control, regardless of where the data is stored. The Convention on Cybercrime (also called the "Budapest Convention") requires each of the more than 60 countries that are party to it[1] to maintain the legal authority to compel companies in their territory to disclose stored electronic data under their control pursuant to valid legal process, with no exception for data the company stores in another country. However, CSPs may also be subject to other countries' laws restricting the disclosure of certain kinds of data, whether because the data is stored in another country or would require action in another

[1] For the official list of countries that are party to the Budapest Convention, see https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=cmPs1otx

country to disclose it, or because the data pertains to another country's citizens. If national laws conflict, CSPs may be forced to choose which country's laws to follow, knowing that they may face consequences for violating another country's laws. Such conflicts pose serious problems for governments seeking data and can frustrate important investigations.

Sometimes such conflict-of-laws problems can be addressed by making a "mutual legal assistance" request to another country, using a system of agreements called "Mutual Legal Assistance Treaties" ("MLATs"). The MLAT system enables law enforcement agencies in one country to seek the assistance of foreign counterparts who can obtain the data. The foreign counterpart reviews a request under its own legal standards and may seek a court order under its law to obtain the data. If the order is granted, the foreign government obtains the data and transmits it to the requesting government. This process has many steps, and depending on the country and the complexity of the request, can take many months to complete.

The number of MLAT requests has increased dramatically in recent years, in light of the massive volume of electronic communications that occur daily over the Internet and the enormous amount of electronic data held by companies located throughout the world. While the MLAT process remains a critical evidence-gathering mechanism, the system has faced significant challenges keeping up with the increasing demands for electronic evidence in criminal investigations worldwide. Moreover, because many CSPs move data among data storage centers in various countries, and split up data into different pieces stored in different locations, it can be difficult both for governments and for the CSPs themselves to know where relevant data is located at any point in time for purposes of sending and fulfilling MLAT requests. The international community thus faces a critical question of how to provide governments efficient and effective access to evidence needed to protect public safety while preserving respect for sovereignty and privacy.

The CLOUD Act

As part of the United States's efforts to address these difficult issues, in March 2018 the U.S. Congress passed the Clarifying Lawful Overseas Use of Data Act, or "CLOUD Act." The CLOUD Act has two distinct parts. *First*, the Act authorizes the United States to enter into executive agreements with other countries that meet certain criteria, such as respect for the rule of law, to address the conflict-of-law problem. For investigations of serious crime, CLOUD agreements can be used to remove restrictions under each country's laws so that CSPs can comply with qualifying, lawful orders for electronic data issued by the other country. *Second*, the CLOUD Act makes explicit in U.S. law the long-established U.S. and international principle that a company subject to a country's jurisdiction can be required to produce data the company controls, regardless of where it is stored at any point in time. The CLOUD Act simply clarified existing U.S. law on this issue; it did not change the existing high standards under U.S. law that must be met before law enforcement agencies can require disclosure of electronic data.

I. CLOUD Act Executive Agreements

The CLOUD Act enables the United States to help its foreign law enforcement partners obtain electronic evidence from global CSPs based in the United States that our partners need for their investigations of serious crime, in a way that we hope and expect will be more efficient and effective than the current legal regime. It authorizes the U.S. government to enter into executive agreements with foreign nations under which each country would remove any legal barriers that may otherwise prohibit compliance with qualifying court orders issued by the other country. Both nations would be able to submit orders for electronic evidence needed to combat serious crime directly to CSPs, without involving the other government and without fear of conflict with U.S. or the other nation's law. Many countries have expressed concern that the MLAT process is not fast enough to provide timely access to electronic data held by global CSPs based in the United States for purposes of their criminal investigations. We anticipate that CLOUD Act agreements will help address some of these concerns and will provide substantial public safety benefits to our foreign law enforcement partners.

- *Many U.S.-based global CSPs currently do not disclose certain electronic data directly to foreign governments conducting criminal investigations.* Foreign governments investigating criminal activities increasingly require access to electronic evidence from companies based in the United States that provide communications services to millions of their citizens and residents. However, many of these U.S.-based global CSPs currently will not disclose electronic data directly to foreign investigating authorities, even if they are served with an order by the foreign authority. These companies are concerned about potential restrictions in U.S. law on disclosure of electronic data and liability if they comply with the foreign orders.

  The potential for conflict of laws exists even when the request from the investigating country involves only communications between non-U.S. persons located abroad and concerns criminal activities occurring entirely outside the United States. Indeed, the only connection to the United States may be that the CSP is headquartered there. When CSPs refuse to comply with orders, foreign law enforcement agencies may find their only viable recourse is the MLAT process, which can be challenging for them to use and is burdened by the increasing volume of requests for electronic evidence in the Internet era.

- *CLOUD Act agreements only remove potential conflicts of law for covered orders.* The CLOUD Act authorizes executive agreements that lift any restrictions under U.S. law on companies disclosing electronic data directly to foreign authorities for covered orders in investigations of serious crime. This would permit U.S.-based global CSPs to respond directly to foreign legal process in many circumstances.

  CLOUD Act agreements, however, do not impose any *new* obligation on U.S.-based global CSPs to comply with a foreign government order; nor does the fact of an agreement establish, by itself, that a foreign government has jurisdiction over that CSP. By the same

token, CLOUD Act agreements do not impose any new obligation on *foreign* CSPs to comply with a U.S. government order; and the fact of an agreement, by itself, does not establish that the U.S. government has jurisdiction over a foreign company. In addition, these agreements do not impose any obligation on either government to compel companies to comply with orders issued by the other. The only legal effect of a CLOUD agreement is to eliminate the legal conflict for qualifying orders. Because the United States currently receives many more requests for electronic data than it submits to other countries, we expect the CLOUD Act will have a more dramatic (and beneficial) impact on foreign requests to the United States than on U.S. requests to foreign partners, at least for the foreseeable future.

- *CLOUD Act agreements require significant privacy protections and a commitment to the rule of law.* The CLOUD Act requires that the agreements include numerous provisions protecting privacy and civil liberties. Orders requesting data must be lawfully obtained under the domestic system of the country seeking the data; must target specific individuals or accounts; must have a reasonable justification based on articulable and credible facts, particularity, legality, and severity; and must be subject to review or oversight by an independent authority, such as a judge or magistrate. Bulk data collection is not permitted. Foreign orders may not target U.S. persons or persons in the United States. Agreements may be used only to obtain information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism. They may not be used to infringe upon freedom of speech. The functioning of each agreement is subject to periodic joint review by the parties to ensure that it is being properly applied. To be clear, the Act does not require foreign partners to adhere to standards that perfectly match the U.S. legal system. However, to be eligible, a country must establish appropriate standards and checks and balances within its legal framework to protect privacy, civil liberties, and human rights. Agreements are reviewed by the U.S. Congress at inception and for renewal every five years thereafter.

- *CLOUD Act agreements will reduce the burden on the MLAT system.* A CLOUD Act agreement would not be the exclusive mechanism for either party to the agreement to obtain electronic data; other mechanisms such as MLATs or domestic orders outside the agreement would remain available. However, CLOUD agreements will reduce the burden on the MLAT system, and remove potential legal conflicts that might otherwise be posed by domestic enforcement of orders, by allowing CSPs to respond directly to covered foreign orders without fear of a conflict between the two parties' laws. Moreover, because fewer U.S. government resources will be needed to process incoming MLAT requests from countries with CLOUD agreements, this should allow the United States to respond to other MLAT requests more expeditiously.

- *CLOUD Act agreements are encryption-neutral.* While CLOUD Act agreements will bring significant benefits to governments investigating or seeking to prevent serious crime, they will not solve all problems related to law enforcement's need for timely access to

electronic evidence. Notably, the agreements will not address challenges posed to law enforcement by end-to-end encryption, where decryption capability is limited to the end user. The CLOUD Act requires that executive agreements be "encryption neutral," neither requiring decryption nor foreclosing governments from ordering decryption to the extent authorized by their laws. This neutrality allows for the encryption issue to be discussed separately among governments, companies, and other stakeholders.

II. Ensuring Lawful Access to Data

In light of the challenges discussed above, it is clear that effective criminal investigations often depend on the investigating country having the authority under its domestic law to obtain electronic data that CSPs subject to its jurisdiction hold, including outside of its borders. Indeed, the entire CLOUD Act executive agreement framework is premised on the notion that both the U.S. and its foreign law enforcement partners will have the authority under their domestic laws to compel production of data held abroad by companies under their jurisdiction. Otherwise, the orders issued under the agreement would not reach such data and the CLOUD Act agreements would be of little practical value to either side.

Accordingly, the second part of the CLOUD Act clarifies that U.S. law requires that CSPs subject to U.S. jurisdiction must disclose data that is responsive to valid U.S. legal process, regardless of where the company stores the data. The Act amended the Stored Communications Act ("SCA"), the federal statute that provides U.S. investigators the authority to require the disclosure of information held by CSPs subject to U.S. jurisdiction, by adding the following sentence: "A provider of electronic communication service or remote computing service[2] shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."

This amendment ensures that U.S. law complies with long-standing international principles already implemented in many countries[3] as required by the Budapest Convention decades ago.

[2] The term "remote computing service" is defined in 18 U.S.C. Section 2711 as "the provision to the public of computer storage or processing services by means of an electronic communications system." The term "electronic communication service" is defined in 18 U.S.C. Section 2510 as: "any service which provides to users thereof the ability to send or receive wire or electronic communications."

[3] Australia, Belgium, Brazil, Canada, Colombia, Denmark, France, Ireland, Mexico, Montenegro, Norway, Peru, Portugal, Serbia, Spain, the United Kingdom, and other countries assert domestic authority to compel production of data stored abroad. See, e.g., Winston Maxwell & Christopher Wolf, A Global Reality: Governmental Access to Data in the Cloud, 2-3 (Hogan Lovells) (updated 18 July 2012) ("Notably, every single country that we examined vests authority in the government to require a Cloud service provider to disclose customer data in certain situations, and in most instances this authority enables the government to access data physically stored outside the country's borders, provided there is some jurisdictional hook, such as the presence of a business within the country's borders.").

The clarification is not novel; it confirms U.S. law's conformity with that of many other countries, and it facilitates international cooperation in ways that are important to our foreign partners:

- ***The amendment ensured clarity by restoring the widely accepted and long-standing understanding of U.S. law.*** The CLOUD Act amendment settled a recent disagreement about the scope of the SCA. Specifically, it addressed a U.S. federal court decision from July 2016 (the *Microsoft* case)[4] which, for the first time, had held that the SCA does not authorize the government to require disclosure of data stored abroad from companies subject to U.S. jurisdiction. After the decision, some CSPs in the United States had refused to comply with U.S. court orders under the SCA to produce data stored on servers abroad. The companies refused to comply even where the court orders concerned investigations of criminal conduct within the United States and involving U.S. citizens. This prevented the government from obtaining data critical to protecting public safety in the United States and abroad.

- ***Most countries require disclosure of data wherever it is stored, consistent with the Budapest Convention.*** Article 18(1)(a) of the Budapest Convention requires each party to the convention to adopt national laws under which relevant authorities can compel providers in their territory to disclose electronic data in their possession or control.[5] This requirement contains no exception for data that a company controls but chooses to store abroad. After the *Microsoft* case, the CLOUD Act clarified U.S. law in a manner that ensures that the United States complies with its obligations under the Convention.

- ***Explicit U.S. authority to obtain data CSPs store abroad restored our ability to fulfill MLAT requests from other governments.*** For a time, the inability of U.S. authorities to obtain data that U.S.-based CSPs accessed from their U.S. headquarters but had stored in servers abroad (because of the *Microsoft* decision) also adversely affected our ability to assist foreign countries to obtain electronic data. Just as the U.S. government could not obtain data that CSPs had stored abroad to pursue our own criminal investigations, we also could not obtain the same data to fulfill MLAT requests from other nations. This substantially crippled those nations' ability to acquire evidence from U.S.-based CSPs that was needed to solve crimes and apprehend criminals in their own countries. Our foreign law enforcement partners were increasingly frustrated by this situation and complained

[4] *Microsoft v. United States*, 829 F.3d 197 (2d Cir. 2016). In that case, the government had served upon Microsoft an SCA warrant that had been approved by an independent judge, who had found probable cause to believe the electronic data sought by the government related to the commission of a narcotics crime. The appellate court held, for the first time since the SCA was enacted in 1986, that the SCA did not require Microsoft to disclose information in its custody and control that it had stored on a server in Ireland. Many other U.S. courts disagreed with this decision, and it was on appeal to the U.S. Supreme Court when the CLOUD Act was enacted, mooting the case.

[5] Article 18(1)(a) of the Budapest Convention obligates each Party to "adopt such legislative and other measures as may be necessary to empower its competent authorities to order a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium."

to the United States. This explicit authority in the CLOUD Act therefore also supports our foreign law enforcement partners, by reviving our longstanding ability to fulfill our partners' MLAT requests for data held by U.S.-based CSPs. By the same token, we expect our foreign partners to be able to fulfill any U.S. MLAT requests seeking data held by their local CSPs regardless of the location of the data.

- *The amendment did not expand U.S. investigative authority.* The CLOUD Act amendment to the SCA does not give U.S. law enforcement any *new* legal authority to acquire data. It merely confirms the scope of requirements under the SCA for CSPs that are subject to U.S. jurisdiction. And, it is worth emphasizing, requirements in the United States for obtaining a warrant for the content of electronic communications are perhaps the toughest in the world and are highly protective of individual privacy. A request to issue a warrant must be submitted to an independent judge for approval. The judge cannot authorize the warrant unless he or she finds that the government has established by a sworn affidavit 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. Further, the warrant must describe with particularity the data to be searched and seized; fishing expeditions to see if evidence exists are not permitted. The strict requirements of U.S. law are one reason some of our foreign law enforcement partners find MLAT requests to the United States so demanding.

- *The amendment did not extend U.S. jurisdiction to any new parties.* Nothing in the CLOUD Act changed the requirement that the United States must have personal jurisdiction over a company in order to require the disclosure of information the company holds. U.S. law limiting jurisdiction over foreign companies is based on constraints in the U.S. Constitution and has been developed by U.S. courts over many years. Personal jurisdiction is most readily established when a company is located in the United States. Whether a foreign company located outside the United States but providing services in the United States has sufficient contacts with the United States to be subject to U.S. jurisdiction is a fact-specific inquiry turning on the nature, quantity, and quality of the company's contacts with the United States. The more a company has purposefully directed its conduct into the United States, the more likely a court will find the company is subject to U.S. jurisdiction. U.S. courts applying this analysis in civil matters involving websites, for example, have focused on how interactive a site is with customers in their jurisdiction, considering factors like the function and mechanics of the website, any specific promotion to customers, solicitation of business through the site, and actual usage by customers. Other countries apply similar principles in assessing their personal jurisdiction over foreign companies, sometimes in ways that are more expansive than is permitted under U.S. law.

Conclusion

The United States enacted the CLOUD Act to address a situation that has become unsustainable. In the Internet age, data location is often not a good basis upon which to ground requests to produce electronic data. In fact, some of the largest global companies now operate networks of storage centers in multiple countries, with the data in near-constant transit, moving between servers and across borders automatically. In this technological environment, it can be impossible for investigating governments to submit multiple MLAT requests to multiple foreign governments to obtain electronic data scattered in multiple countries, especially when the governments (and sometimes even the CSPs themselves) do not know where the data is stored and when the data may well have been moved to another location by the time the requests are reviewed. The current situation undermines our foreign partners' efforts to protect the safety of their citizens, just as it undermines U.S. efforts to protect Americans. Nations must ensure that law enforcement officials have reasonable legal authorities to compel production of electronic data that a CSP controls but that may be located in other countries. At the same time, nations also have legitimate interests in protecting data from other governments that do not adhere to appropriate legal standards or abuse their authority for illicit purposes. The challenge is to ensure that government powers to compel production of electronic data are exercised and overseen in a way that respects the rule of law, protects privacy and human rights, and appropriately reduces conflicts between the laws of the countries concerned. Failing to address this situation would increase incentives for data localization across the world, which would harm both global commerce and public safety. A framework of executive agreements among rights-respecting countries under the CLOUD Act will support those countries' efforts to investigate serious crime—efforts that are vital to protecting our societies and keeping our citizens safe.

Additional Resources (click to view)

Full text of the CLOUD Act.

Remarks of Richard W. Downing, U.S. Deputy Assistant Attorney General, at the Academy of European Law, London, U.K., "Prospects for Transatlantic Cooperation on the Transfer of Electronic Evidence to Promote Public Safety" (April 5, 2019).

Remarks of Sujit Raman, U.S. Associate Deputy Attorney General, at the Center for Strategic and International Studies, Washington, D.C., "Toward a New Paradigm on Cross-Border Data Flows: Moving Ahead with the CLOUD Act" (May 24, 2018).

Thomas P. Bossert & Paddy McGuinness, "Don't Let Criminals Hide Their Data Overseas," N.Y Times (February 14, 2018).

Statement of Richard W. Downing, U.S. Deputy Assistant Attorney General, before the U.S. House of Representatives Committee on the Judiciary (June 15, 2017).

Statement of Brad Wiegmann, U.S. Deputy Assistant Attorney General, before the U.S. Senate Committee on the Judiciary's Subcommittee on Crime and Terrorism (May 24, 2017).

Written Testimony of Paddy McGuiness, U.K. Deputy National Security Advisor, before the U.S. Senate Committee on the Judiciary's Subcommittee on Crime and Terrorism, at a Hearing entitled "Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights" (May 24, 2017).

Frequently Asked Questions

A. Purpose of the CLOUD Act

1. What was the purpose of the CLOUD Act?

The United States enacted the CLOUD Act to improve procedures for both foreign and U.S. investigators in obtaining access to electronic information held by service providers. Such information is critical to investigations of serious crime by authorities around the world, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime.

While the United States has faced serious issues in accessing such information to protect public safety, the need is even greater for our foreign partners because so much information is held by companies based in the United States. In recent years, the number of mutual legal assistance requests seeking electronic evidence from the United States has increased dramatically, straining resources and slowing response times. Foreign authorities have relatedly expressed a need for increased speed in obtaining this evidence. In addition, many of the assistance requests the United States receives seek electronic information related to individuals or entities located outside the United States, and the only connection of the investigation to the United States is that the evidence happens to be held by a company based in our nation.

The CLOUD Act updates 20th century legal frameworks to respond to the revolution in electronic communications and recent innovations in the way global technology companies configure their systems. The Act permits our foreign partners that have robust protections for privacy and civil liberties to enter into executive agreements with the United States to use their own legal authorities to access electronic evidence in order to fight serious crime and terrorism. The CLOUD Act thus represents a new paradigm: an efficient, privacy-protective approach to public safety by enhancing effective access to electronic data under existing legal authorities. This approach makes both the United States and its partners safer while maintaining high levels of protection of privacy and civil liberties.

The CLOUD Act also clarified the U.S. Stored Communications Act to enable the framework envisioned by the CLOUD Act, that each nation would use its own law to access data. The CLOUD Act clarified that U.S. law requires that providers subject to U.S. jurisdiction disclose data that is responsive to valid U.S. legal process, regardless of where the company stores the data. This ensured consistency with U.S. obligations under Article 18(1) of the Budapest Cybercrime Convention, aligning the United States with the more than 60 other parties to the Convention.

B. CLOUD Act Agreements

2. Who can enter into a CLOUD Act agreement with the United States?

The CLOUD Act provides that the United States may enter into CLOUD Act agreements only with rights-respecting countries that abide by the rule of law. In particular, before the United States can enter into an executive agreement anticipated by the CLOUD Act, the CLOUD Act requires that the U.S. Attorney General certify to the U.S. Congress that the partner country has in its laws, and implements in practice, robust substantive and procedural protections for privacy and civil liberties, based on factors such as:

- adequate substantive and procedural laws on cybercrime and electronic evidence, such as those enumerated in the Budapest Convention;
- respect for the rule of law and principles of nondiscrimination;
- adherence to applicable international human rights obligations;
- clear legal mandates and procedures governing the collection, retention, use and sharing of electronic data;
- mechanisms for accountability and transparency regarding the collection and use of electronic data; and
- a demonstrated commitment to the free flow of information and a global Internet.

3. How do CLOUD Act agreements relate to Mutual Legal Assistance (MLA) Treaties?

The CLOUD Act supplements rather than eliminates MLA, which remains another method by which evidence in criminal cases is made available to authorities from other countries. MLA will continue to be an option to obtain data that is not covered by such an agreement, as well as in the absence of such an agreement. As CLOUD Act agreements increase the efficiency of many requests for data, the United States should also be able to process MLA requests more quickly due to the decrease in volume, benefiting all partners regardless of whether the requesting country itself has a CLOUD Act agreement.

4. How do CLOUD Act agreements reduce conflicts of laws between countries?

Both the United States and any partner in a CLOUD Act agreement would agree to remove legal restrictions to providers' compliance with orders issued under the agreement in circumstances both countries find appropriate. As a result, countries that enter into CLOUD Act agreements will be able to use familiar domestic legal process to authorize access to data with the assurance

that the other party's law will not be a barrier to compliance with their lawful order. The types of orders that may be issued under the agreement must be mutually agreed with full consideration of the interests of both countries.

5. How is law enforcement access to data different under a CLOUD Act agreement?

Under a CLOUD Act agreement, a party has an alternative to the MLA process to obtain the disclosure of data held by a provider over whom it has jurisdiction. Because the agreement requires each country to remove legal restrictions to provider compliance with orders issued by the other country, the authorities of each country may use their own domestic authority to require disclosure with confidence that the legal demand will not violate the other country's law.

6. If a foreign country enters into a CLOUD Act agreement, could the United States then use the agreement to target data concerning that country's nationals? And could the foreign country use the agreement to target data concerning U.S. nationals?

The CLOUD Act requires that foreign government orders that are subject to an executive agreement may not intentionally target data of U.S. persons or persons located in the United States. The foreign government is free in negotiations to seek similar restrictions that would prevent the United States from using orders subject to the agreement to target data of its nationals or residents. The U.S. and other countries may continue to use their existing legal process to seek data outside CLOUD Act agreements, but may continue to face a conflict of laws in those circumstances.

7. Must legal process issued by another country under a CLOUD Act agreement conform to the requirements for U.S. legal process? For example, must a partner demonstrate "probable cause" in order to obtain content?

No. The legal process issued by a country under a CLOUD Act agreement does not have to conform to the requirements of U.S. law. Instead, the legal process must conform to the requirements of that country's domestic law for the data sought. This means, for example, that if two U.K. residents are communicating with each other in the course of committing a crime, but the data is stored by a provider based in the U.S., a U.K. order, rather than a U.S. warrant, can be used to obtain the evidence directly from the provider (assuming the U.K. otherwise has jurisdiction over that provider).

8. Must legal process issued by another country under a CLOUD Act agreement first be submitted to the U.S. government before it is served on a provider?

No. When proceeding under a CLOUD Act agreement, the foreign authorities may serve their domestic legal process directly on providers in accordance with their own law, and providers may disclose responsive data directly to the foreign authorities.

9. *What types of data are available to the U.S. and other countries pursuant to CLOUD Act agreements?*

CLOUD Act agreements concern data stored or processed by communications service providers. Such data could include the contents of communications, non-content information associated with such communications, subscriber information, and data stored remotely on behalf of a user ("in the cloud").

While CLOUD Act agreements may cover both access to stored content and non-content and ongoing acquisition of communications in real time, there is no requirement that any particular agreement cover all such access.

10. *Will CLOUD Act agreements cover civil, administrative, or commercial inquiries? Can they be used for spying on another country?*

No. CLOUD Act agreements are only used to obtain information relating to the prevention, detection, investigation, or prosecution of serious crime and only in response to legal process.

11. *How do CLOUD Act agreements enhance privacy?*

We expect the high standards required for eligibility for CLOUD Act agreements to be a significant motivation for countries to increase protections for privacy and civil liberties. The CLOUD Act requires that countries wishing to enter into executive agreements with the United States have in place rigorous standards for the issuance of legal process. While countries are not required to have the exact same requirements as United States law, the Act explicitly requires that covered foreign orders must be subject to independent review or oversight, be based on a reasonable justification grounded in credible and articulable facts, and identify a specific person, account, or other identifier. These procedural and substantive requirements ensure a solid legal and factual basis before investigators require disclosure of private communications. Moreover, the foreign government's laws must also protect from arbitrary and unlawful interference with privacy and must provide for procedures subject to effective oversight that govern how its authorities collect, retain, use, and share data. The foreign government must provide accountability and appropriate transparency about the collection and use of electronic data. To be eligible, some countries interested in executive agreements will likely need to increase standards and improve procedures.

12. *Do CLOUD Act agreements allow the U.S. government to acquire data that it could not before?*

No. CLOUD Act agreements remove the possibility that one party's legal restrictions on disclosing data could conflict with the other party's legal authority to collect evidence. CLOUD Act agreements do not alter the fundamental constitutional and statutory requirements U.S. law enforcement must meet to obtain legal process for that data – standards that are among the most privacy-protective in the world.

13. Do CLOUD Act agreements impose U.S. law on other countries?

No. To the contrary, the CLOUD Act affords respect to the laws of other countries, allowing partners to obtain authority under their own law and setting out a means to address partners' restrictions on disclosure. Foreign partners obtain legal authority under their own law, and foreign law need not match the legal standard applicable to U.S. authorities—though it must nevertheless provide adequate protections for privacy and civil liberties. Moreover, the CLOUD Act does not expand the jurisdiction of the United States, nor do CLOUD Act agreements create new obligations under U.S. law for service providers.

14. How would an order subject to a CLOUD Act agreement be enforced? Can a provider being ordered to disclose information challenge such authority?

There is no requirement under U.S. law that a provider comply with a foreign order, and the CLOUD Act creates no such requirement. Any enforcement must be conducted under the law of the country requiring the disclosure. A U.S.-based provider receiving a foreign order to disclose information can challenge the order under the foreign country's law to the extent such a challenge is permitted by that law. Because any legal prohibition on disclosing data in response to a foreign order that is subject to the agreement will have been removed, a foreign court enforcing the order will not need to consider comity interests or other burdens that might otherwise arise from a conflict of laws.

15. If a provider receives legal process subject to a CLOUD Act agreement and suspects that the legal process may not satisfy the requirements of the CLOUD Act, what can it do?

In the event the provider has concerns about the applicability of the agreement to a particular production order, it can consult with the designated authority of the country issuing the order. In addition, the designated authority of the other country has the ability to render the agreement inapplicable in a particular case if it believes the agreement is improperly invoked.

16. When is the account holder notified of an order issued under a CLOUD Act agreement?

CLOUD Act agreements do not create any obligations or restrictions on providers; they simply remove legal restrictions that would otherwise conflict with compliance with covered orders. Providers issued orders covered by a CLOUD Act agreement are subject to the domestic requirements of the issuing country, and the issuing country's law governs whether or how notice to an account holder by the provider may be prohibited.

C. Amendments to the Stored Communications Act

17. Does the amendment of the Stored Communications Act in the CLOUD Act create new authority for U.S. law enforcement to obtain information?

No. The clarification of the Stored Communications Act in the CLOUD Act restores certainty under United States law to ensure its consistency with long-standing practice and U.S. treaty obligations under the Budapest Convention. U.S. law enforcement uses existing legal authority to require the disclosure of data from companies already subject to U.S. law by meeting the traditional legal standards – standards that are among the most privacy-protective in the world.

18. What data is subject to a warrant under the Stored Communications Act?

The CLOUD Act does not create any new form of warrant. It simply clarifies the obligations under the Stored Communications Act of providers subject to U.S. jurisdiction, including obligations to disclose information pursuant to warrants. A warrant may require the disclosure of content of communications and all records and other information pertaining to a customer or subscriber of a provider. Under U.S. constitutional law, law enforcement must meet high standards to obtain a warrant and warrants may only permit searches of particular places for particular things.

19. What is necessary under the Stored Communications Act to obtain a warrant for stored content?

The Stored Communications Act permits law enforcement to obtain a warrant to require a provider to disclose the stored contents of a user account. Warrants must meet demanding and highly privacy-protective constitutional requirements. The warrant must be supported by a statement sworn under penalty of perjury showing probable cause that the place searched will contain particular things subject to seizure; must state with particularity the crime that is alleged, the information to be disclosed and the evidence to the seized; and must be approved by an independent judge. The CLOUD Act did not change these existing high standards under U.S. law. "Probable cause" is a particularly exacting standard, among the most demanding in the world.

20. Will a warrant issued under the Stored Communications Act allow the U.S. to scoop up large amounts of data indiscriminately?

No. The CLOUD Act did not alter or expand the historical scope of warrants issued under U.S. law. Indiscriminate or bulk data collection is not permitted.

21. Does the amendment of the Stored Communications Act in the CLOUD Act allow the United States to unilaterally obtain foreign nationals' data held overseas?

Just as in many other countries, and as required by the Budapest Convention, U.S. law provides that companies subject to U.S. jurisdiction may be compelled, pursuant to a court order, to produce data subject to their control regardless of where the data is stored. That data could potentially be about non-U.S. nationals, if the stringent requirements of U.S. law are met. Where

no CLOUD Act agreement is in place, a company's compliance with a U.S. court order might conflict with a foreign country's law forbidding production of data. In such cases, the U.S. government could elect to pursue alternate channels, such as narrowing or modifying a request to avoid the conflict; resolving the conflict through closer inquiry or good-faith negotiation; or making the request under an applicable MLAT. Should the U.S. government seek to enforce the order notwithstanding a conflict with foreign law, U.S. courts can be expected to apply long-standing U.S. and international principles regarding conflicts of law to ensure appropriate respect for international comity by applying a multi-factor balancing test, taking into account the interests of both the United States and the foreign country.

22. Does data ownership impact whether U.S. law enforcement can obtain data from a provider?

U.S. law related to law enforcement access to data, including under the provision amended by the CLOUD Act, does not turn on the question of data "ownership." Instead, fully consistent with the Budapest Convention, United States law can require the disclosure of data in a provider's possession or control. This focus on possession or control is consistent with paragraph 173 of the Explanatory Report to the Budapest Convention, which states:

> The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory. . .

23. What types of providers are subject the Stored Communications Act?

The provisions relating to the preservation and disclosure of data by providers are applicable only to providers of "remote computing service[s]" ("RCS") and "electronic communication service[s]" ("ECS"). RCS and ECS are defined by U.S. law. See 18 U.S.C. § 2510(15) ("'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications"); id. § 2711(2) ("'remote computing service' means the provision to the public of computer storage and processing services by means of an electronic communications system").

These definitions include such companies as email providers, cell phone companies, social media platforms, and cloud storage services. They do not include a company just because it has some interaction with the Internet, such as certain e-commerce sites.

These definitions are consistent with Article 1.c. of the Budapest Convention, which covers "any public or private entity that provides to users of its service the ability to communicate by means of a computer system" and "any other entity that processes or stores computer data on behalf of such communication service or users of such service."

24. Who is subject to the requirements of the Stored Communications Act? Is it only U.S. corporations, U.S.-headquartered corporations, or U.S.-owned companies? Does a warrant under the Stored Communications Act apply to a company located outside the United States but which provides its services within the territory of the U.S.?

The CLOUD Act did not give U.S. courts expanded jurisdiction over companies. Its amendment to the Stored Communications Act merely clarified the obligations of those providers who are already subject to U.S. jurisdiction by confirming that they are obliged to disclose responsive data within their possession or control, regardless of where it is stored.

In order to place legal requirements on a provider, the provider must be subject to U.S. jurisdiction. U.S. jurisdiction is not limited to U.S. corporations, U.S. headquartered companies, or companies owned by U.S. persons. But neither is U.S. jurisdiction unlimited.

United States requirements for exercising jurisdiction over a person are often more stringent than those in the law of other countries. Whether a company providing services in U.S. territory is subject to U.S. jurisdiction is a highly fact-dependent analysis regarding whether the entity has sufficient contacts with the U.S. to make the exercise of jurisdiction fundamentally fair. The more a company has purposefully availed itself of the privilege of conducting activities in the United States or purposefully directed its conduct into the U.S., the more likely a U.S. court is to find that the company is subject to U.S. jurisdiction.

25. Does a warrant under the Stored Communication Act apply to data stored by a U.S. company's subsidiary that is incorporated or headquartered in another country?

The CLOUD Act does not alter traditional requirements for jurisdiction over an entity with possession or control over data. The analysis remains the same regardless of corporate structure. The United States court must have jurisdiction over an entity that has possession or control over data in order to require its disclosure. Whether a company exercises sufficient control over data held by a subsidiary is a fact-dependent inquiry.

26. Will U.S. law enforcement go directly to service providers to obtain information of an employee of an enterprise when the enterprise is not otherwise suspected of committing a crime?

The CLOUD Act does not change U.S. law or practice with regard to enterprise customer data. The U.S. Department of Justice's Computer Crime and Intellectual Property Section has publicly advised that "prosecutors should seek data directly from the enterprise, if practical, and if doing so will not compromise the investigation. Therefore, before seeking data from a provider, the prosecutor, working with agents, should determine whether the enterprise or the provider is the better source for the data being sought." For more information about the factors that influence the Department's approach to seeking enterprise data, see: https://www.justice.gov/criminal-ccips/file/1017511/download.

27. Does the United States use the Stored Communications Act to obtain trade secrets of foreign corporations from service providers for the purpose of benefiting U.S. companies?

No. The United States has championed the international norm that no government should in any way conduct or support the theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to its companies or commercial sectors. See: https://www.esteri.it/mae/resource/doc/2017/04/declaration_on_cyberspace.pdf (G7 Declaration on Responsible States Behavior in Cyberspace). Under U.S. law, theft of trade secrets is subject to criminal prosecution with penalties of up to ten years in prison.

28. When a court order is issued by the United States pursuant to the Stored Communications Act, when is the account holder notified of the search?

Providers may notify account holders of searches pursuant to a U.S. court order under the Stored Communications Act unless an independent judge has issued a protective order. Protective orders relating to all Stored Communications Act orders (not just those for orders pursuant to CLOUD Act agreements) are issued when the independent judge determines that there is reason to believe that notification of the existence of the court order may create the adverse result of (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial. Under U.S. Department of Justice policy, such orders must generally be limited to one year.

29. Does the CLOUD Act require providers to decrypt data in response to law enforcement requests?

No. The CLOUD Act is "encryption neutral." It does not create any new authority for law enforcement to compel service providers to decrypt communications. Neither does it prevent service providers from assisting in such decryption, or prevent countries from addressing decryption requirements in their own domestic laws.