

## 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 be 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](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.