

CLOUD Act: Answers to Frequently Asked Questions

July 2025

[Jennifer Daskal](#) & [Richard Salgado](#)¹

These Frequently Asked Questions (FAQs) update [FAQs](#) from 2019, about the meaning and implications of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). These updated FAQs reflect developments of the past several years, and, like the earlier FAQs, are intended to help address some outstanding questions about the CLOUD Act.

1. At a high level, what did the CLOUD Act do?

The CLOUD Act amended three key U.S. surveillance statutes: the Stored Communications Act (SCA), the Wiretap Act, and the Pen Registers and Trap and Trace Devices Statute (“Pen/Trap statute”).

The three key changes are as follows:

First, the CLOUD Act amended the SCA to specify that service providers subject to the SCA are required to comply with lawful demands under the SCA to preserve or disclose stored data in their possession, custody, or control, regardless of the location of the data. See 18 U.S.C. § 2713. More about this in Section I below.

Second, the CLOUD Act added new exceptions² to the prohibitions³ on service providers from disclosing user data to foreign governments.

¹ The views expressed here are solely those of the authors. The authors express their thanks for comments on earlier drafts from participants in the Cross Border Data Forum.

² The CLOUD Act added three exceptions: one in the SCA; one in the Wiretap Act; and one in the Pen/Trap statute. The exception to the prohibition in the SCA is found at 18 U.S.C. §§ 2702(b)(9) & (c)(7). In the Wiretap Act, it is found at 18 U.S.C. § 2511(2)(j). In the Pen/Trap statute, it is found at 18 U.S.C. § 3121(a), although not technically described as an “exception” in that statute.

³ The SCA states that a covered service provider “shall not divulge” stored communications content to “any person or entity,” unless pursuant to specified statutory exceptions. See 18 U.S.C. § 2702(a) & (b). The Wiretap Act similarly prohibits interception, use or disclosure of

These exceptions apply only if the requesting foreign government has entered into an executive agreement with the United States, in accordance with specified statutory requirements. (The United Kingdom and Australia were the first to enter into such executive agreements.) See 18 U.S.C. § 2523. More about this in Section II below.

Third, the CLOUD Act gave service providers a new statutory right, based on international comity, to object to SCA legal process seeking content in certain situations. See 18 U.S.C. § 2703(h). More about this in Section III below.

I. Amendment to the Stored Communications Act: Disclosure Obligations in Response to Lawful Production Orders

The CLOUD Act amended the SCA to provide that service providers subject to the SCA are required to comply with lawful demands under the SCA to preserve or disclose stored data in their possession, custody, or control, regardless of the location of data. See 18 U.S.C. § 2713.

2. What did this part of the CLOUD Act do?

The CLOUD Act specifies that a provider with possession, custody or control of user information can be compelled to preserve, backup, or disclose the information if required by the SCA, regardless of where that data is stored. In so doing, it [resolved a dispute](#) that was pending at the time before the Supreme Court of the United States between the U.S. government and Microsoft about whether U.S. law enforcement could, pursuant to a search warrant issued under the SCA, compel Microsoft to disclose data in Microsoft's possession, custody and control, but stored on servers located in Ireland.

This did not create any new authority to compel production of data under the SCA and did not change any other surveillance statute.

electronic communications, absent specified exceptions. See 18 USC § 2511. The Pen /Trap statute prohibits the use of a pen register or trap and trace device unless an exception applies. 18 U.S.C. § 3121(a).

3. Did the CLOUD Act change the standards by which governmental entities in the U.S. can compel providers to disclose user data?

No.

The Act did not change the process or standards by which governmental entities in the U.S. can seek to compel the production of data from service providers. It also did not change the type of provider potentially subject to such an order.

Governmental entities in the United States must obtain a warrant to obtain communications content in the hands of a service provider. This was true both before and after the CLOUD Act.

4. Did the CLOUD Act give governmental officials in the U.S. extraterritorial power over providers outside the U.S.?

No. The CLOUD did not change the requirement that the government must have jurisdiction over the provider before it could employ the SCA to compel the provider to preserve or disclose data under the SCA. The U.S. government has [acknowledged](#) this.

5. Did the CLOUD Act change how a provider can challenge a demand made under the SCA?

Yes. As discussed in Section III that follows, the CLOUD Act gave providers a new statutory right, based on international comity, to object to SCA legal process seeking content in certain situations.

It did not otherwise change or eliminate any of the otherwise available grounds for objecting to legal process under the SCA or common law.

II. The CLOUD Act and US Blocking Statutes

The CLOUD Act amended the SCA, the Wiretap Act, and the Pen/Trap statute to add in each a new exception to the provisions that otherwise can prohibit a service provider from disclosing user data to a foreign government. The exceptions to these so-called “blocking statutes” are

available where the foreign government has an executive agreement in place that satisfies the requirements specified in the CLOUD Act.

The CLOUD Act limits the availability of these executive agreements to countries with laws that protect privacy and civil liberties, among other requirements. The Act also requires that such agreements contain numerous conditions on the foreign government when invoking an agreement. These include that the agreement is to be used only for purposes relating to serious crime and not to infringe on free speech, and the foreign government cannot intentionally target the data of Americans or anyone located in the United States.

Where there is such an agreement in place, service providers may disclose the data requested by a foreign government pursuant to the agreement without running afoul of the blocking statutes that might otherwise apply.

6. How does the CLOUD Act address so-called “blocking statutes”?

The SCA, Wiretap Act and Pen/Trap statute prohibit a provider covered by those laws from disclosing user data, including disclosures to foreign governments, unless a specific exception set out in the statute applies. These provisions are often referred to as “blocking statutes.” Many countries have versions of such statutes.⁴

The CLOUD Act creates an exception to these restrictions in the limited circumstances in which the disclosure request to the service provider comes from a country with which the U.S. has a special executive agreement in place. This sort of agreement is often referred to as a “CLOUD Act Agreement” or “Data Access Agreement.”

⁴ See Matt Perault and Richard Salgado, [Untapping the Full Potential of CLOUD Act Agreements](#), Center for Strategic and International Studies (June 6, 2024) (“In the European Union, Article 48 of the General Data Protection Regulation serves to restrict data disclosure to non-EU member governments unless certain criteria are satisfied. France also has a blocking statute prohibiting the disclosure of information that would harm French interests.”)

7. What is a CLOUD Act agreement?

A CLOUD Act agreement, also sometimes called a “Data Access Agreement”, is an executive agreement between the U.S. and another sovereign (either a foreign country or international body like the European Union), that satisfies the requirements in the statute. To qualify for a CLOUD Act agreement with the United States, a foreign country must meet certain standards. The CLOUD Act also requires that the agreements themselves contain certain features, protections and limitations.

Notably, a foreign government is precluded from using the agreement to intentionally target U.S. citizens, permanent legal residents and others in the United States; such governments can use the agreement to target foreigners located outside the United States only. This, and other limitations, are discussed more below.

8. What are the requirements that a foreign government must meet to be eligible for a CLOUD Act agreement?

The CLOUD Act sets forth substantive and procedural protections that foreign governments must adhere to, along with several other conditions designed to ensure protections for privacy and civil liberties, and respect for human rights.

Among other preconditions, the CLOUD Act requires a written certification by the Attorney General, with concurrence of the Secretary of State, that the foreign government affords substantive and procedural protections for privacy and civil liberties; has mechanisms in place to protect the data of U.S. persons; and adheres to international human rights standards. Only those countries that demonstrate respect for privacy, freedom of expression, fair trial rights, and prohibitions on arbitrary detention are eligible for CLOUD Act agreements.

9. Does the CLOUD Act require certain agreement provisions?

Yes. The statute lays out many requirements for the content of the agreements themselves. These include criteria for requests made pursuant to agreements. Among other criteria, they must be subject to review or oversight by a court or other independent authority, issued for a purpose relating to serious crime, and contain limits on who can be targeted and how data is handled, as discussed in more details below.

10. Have any CLOUD Act agreements been put in place?

Yes. The first two such executive agreements were with the [United Kingdom](#) and [Australia](#). The CLOUD Act provides that any agreement will expire after five years but may be renewed if the U.S. attorney general and secretary of state certify to Congress that the other country still satisfies the statutory requirements.

11. In what type of investigations can CLOUD Act agreements be used?

Requests under CLOUD Act agreements must be for the purpose of obtaining information related to the prevention, detection, investigation or prosecution of serious crime, such as terrorism. They may not be used to infringe freedom of speech. They cannot be used for bulk collection of user data.

12. Can a foreign government intentionally target United States Persons or those located in the U.S. using a CLOUD Act agreement?

No. The CLOUD Act specifies that a foreign government may not intentionally target a United States person or a person located in the United States. The Act defines “United States Person” as “a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States.”

In addition, the foreign government is prohibited from targeting a non-United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States.

13. What happens if a foreign government inadvertently obtains data about United States Persons?

The underlying statute requires that foreign countries adopt appropriate provisions to minimize the acquisition, retention and dissemination of data obtained under a CLOUD Act agreement concerning United States persons. Both of the first two CLOUD Act agreements, one with the U.S. and one with Australia, set out steps to deal with inadvertently obtained data about United States Persons.

In addition, a foreign government may not target a non-United States person in order to obtain information about a United States person using the agreement.

14. Can a foreign government use a CLOUD Act agreement on behalf of other governments?

No. Under the CLOUD Act, executive agreements may not be used to obtain information at the request of any other government.

15. Are requests made by a foreign government under a CLOUD Act agreement necessarily compulsory, requiring a provider to comply?

No. The fact that a request is made to a provider pursuant to the CLOUD Act agreement does not mean that compliance by the provider is compulsory. The CLOUD Act and associated agreement create an exception to otherwise applicable prohibitions (the blocking statutes discussed above) that could prevent a service provider from lawfully disclosing the requested data. They do not create an affirmative basis for a foreign government to compel a provider to disclose such data. In fact, providers can and do resist such requests for data, as suggested in provider transparency reports.

16. Can the CLOUD Act be used to compel a service provider to decrypt data or otherwise change its encryption practices?

No. The CLOUD Act specifically states that a CLOUD Act agreement “shall not create any obligation that providers be capable of decrypting data.” It similarly prohibits the imposition of any limitations that prevent providers from decrypting data.

17. Does a CLOUD Act agreement change how governmental agencies in the U.S. can compel a service provider to disclose user data?

No. The rules under U.S. law governing when and how governmental agencies in the U.S. can compel a provider to disclose user data are the same whether or not a CLOUD Act agreement is in place.

18. What happens if a government violates the terms of a CLOUD Act agreement?

There are several possible ways to respond to a violation of a CLOUD Act agreement.

Both the U.S.-U.K. and U.S.-Australia agreements include provisions that enable any party to terminate the agreement at any point, by sending a diplomatic note to the other party. Termination is automatic, one month after such notice. Those agreements also specify that if either party concludes that the agreement may not properly be invoked with respect to any order, that party can let the other know, and the agreement can't be used for that order. The U.S.-UK agreement also has an additional provision that allows either party to prohibit the invocation of the agreement with respect to an identified category of orders.

In addition, under the terms of the CLOUD Act, all foreign governments with which there is a CLOUD Act agreement must agree to periodic reviews of compliance, conducted by the United States. Both the U.S.-U.K. and U.S.-Australia agreements have made this requirement reciprocal.

III. Statutory Comity-Based Mechanism to Challenge U.S. Legal Process

The CLOUD Act amended the SCA to add a new statutory basis on which a service provider can object to legal process issued under the SCA to compel the service provider to disclose content, in certain situations, to serve the interests of justice and international comity.

19. How does the CLOUD Act's new statutory comity objection work?

The CLOUD Act adds a new statutory basis for a service provider to object to SCA legal process seeking the content of a customer or subscriber if the provider reasonably believes the (i) customer or subscriber is not a U.S. person and does not reside in the U.S., and (ii) disclosure would create a material risk of violating the laws of a foreign government with which the U.S. has a CLOUD Act agreement.

After giving the government an opportunity to respond to the objection, a court may modify or quash the legal process if it finds that (i) the disclosure would violate the laws of such a foreign government, (ii) the interests of justice, including specific considerations of international comity, dictate modifying or quashing the legal process, and the customer or subscriber is not a U.S. person and does not reside in the U.S.

20. Is this the only situation in which a provider can raise a comity objection?

No. The CLOUD Act says that the addition of this statutory basis for objecting based on comity grounds does not preclude a provider from raising a comity objection founded in the common law in other settings. [CLOUD Act](#), § 103(c) (Rule of Construction).