Business Software Alliance

What Is the CLOUD Act?

The Clarifying Lawful Overseas Use of Data (CLOUD) Act amended the Electronic Communications Privacy Act (ECPA), which is the US statute governing how law enforcement agencies may obtain information held by certain technology companies, including cloud service providers.[1] The CLOUD Act was passed into law on March 23, 2018.[2]

The CLOUD Act has two parts. The first part clarifies that orders issued under the existing statutory framework in ECPA can reach data regardless of where that data is stored.[3] The second part creates a new framework for government-to-government agreements to govern cross-border law enforcement requests.[4] The United States has entered into two such agreements, with the United Kingdom in 2019 and with Australia in 2021.

When Can Data Be Sought From Technology Companies Under the CLOUD Act?

Law enforcement agencies use a warrant to obtain a user's digital content. A warrant may only be issued in a criminal investigation—and only when an independent court finds that a series of constitutional and statutory safeguards are met.[5]

Digital content may be sought from technology providers:

- Only in criminal investigations
- Only after obtaining a warrant approved by an independent court
- Not in national security investigations

The CLOUD Act does not authorize bulk requests.

- Digital content can only be sought from technology providers with a warrant, which must be issued by an independent court. A warrant may only seek data that is identified with particularity in the warrant itself; the warrant must be approved by an independent court.

ORDERS FOR DIGITAL CONTENT MUST SATISFY LEGAL REQUIREMENTS

All of the following requirements must be satisfied when digital content is sought under the CLOUD Act:

- The law enforcement agency must be investigating a crime.
- The law enforcement agency must apply to a court for a warrant.
- The law enforcement officer must swear to the facts in the warrant application.
- The warrant application must describe—with particularity—the information sought.
- An independent court must find that the warrant application establishes probable cause that the information to be searched contains evidence of a specific crime.

Enterprise data is subject to additional safeguards:

- When digital content belongs to an enterprise, rather than an individual, the US Department of Justice has committed to "seek data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation."[6]
- This commitment recognizes that in many cases, the enterprise customer—and not the cloud provider—will be the appropriate entity to respond to legal process.

What Are the Requirements for Issuing an Order Under the CLOUD Act?

Most types of data—including the content of communications—may only be obtained under the CLOUD Act after an independent court has found that specific statutory requirements are met.[7]

To obtain digital content, law enforcement must obtain a warrant, which is issued by an independent court. This process is subject to a range of constitutional, statutory, and procedural safeguards under US law.

THERE ARE THREE CRITICAL STEPS:

1. **APPLICATION: A law enforcement officer must submit a warrant application to an independent court.** The application must include facts establishing that the information sought contains evidence of a crime—and describe with particularity the information to be obtained. The officer submitting the warrant application must swear to those facts.

2. **COURT APPROVAL: An independent court must determine that probable cause exists.** A warrant may only be issued when a prosecutor has convinced a court that probable cause exists that a specific crime has occurred or is occurring and that the place to be searched, such as an email account, contains evidence of that specific crime. This finding is made by an independent court and not by the law enforcement authority itself.

3. **ABILITY TO CHALLENGE: Once issued, technology companies may challenge an order and raise conflicts of law.** Technology companies may challenge an order in court by filing a motion to modify or quash the order with the issuing court.[8] Indeed, the CLOUD Act specifically preserves the ability of providers to bring common law "comity challenges" if an order conflicts with a foreign country's law.[9] Courts evaluate such challenges under a range of factors, including the degree of specificity of the request, whether the information sought originated in the US, and whether the information could be obtained through alternative means.[10]

These requirements impose important restrictions on orders for digital content. Providers that furnish digital content to a US government agency in the absence of a search warrant that meets these standards risk civil and criminal liability.[11]

Orders can seek data from technology providers headquartered outside the US.

- The CLOUD Act governs the issuance of orders to broad categories of technology providers.[12]
- Those technology providers may be subject to an order under the CLOUD Act if they are subject to US jurisdiction and have the technical ability to access the data sought—regardless of where the provider is headquartered, services are rendered, or data is stored.[13] The location of a company's headquarters and the location in which data is stored are not determinative.
- Many companies based outside the US are subject to US jurisdiction, such as when a company has operations or offices in the US or enters into contracts with US customers.[14]

What Is a Warrant?

US law enforcement agencies use warrants to obtain digital content. Warrants are subject to strict safeguards and may only be issued if a court finds that a law enforcement officer has shown there is probable cause to believe the information sought will contain evidence of a crime.

Who issues a warrant? Courts issue warrants. This ensures that a neutral and detached judge, and not just the law enforcement agency seeking the warrant, approves the requested search.

Where do the requirements to issue a warrant come from? The United States Constitution, statutes, and procedural rules all impose privacy-protective requirements on warrants. Under the Fourth Amendment to the US Constitution, warrants may only be issued (1) upon a showing of probable cause, (2) when supported by oath or affirmation, (3) when they particularly describe the places to be searched and things to be seized. Federal statutes like ECPA further limit the situations in which law enforcement agencies may seek a warrant. In addition, the Federal Rules of Criminal Procedure contain additional safeguards limiting how courts may issue warrants.

Can warrants approve bulk collection? No. Warrants are issued in particular criminal cases to obtain specific types of data that are identified with particularity in the warrant itself. The Fourth Amendment of the US Constitution requires a warrant to describe with particularity the place to be searched, and the persons or things to be seized, ensuring the search will be carefully tailored to its justifications.

US COURTS: INDEPENDENT REVIEW

The United States Constitution establishes the judicial branch (courts) as one of three separate and distinct branches of the federal government.[15] The other two branches are the executive branch (led by the President) and the legislative branch (Congress). Under this separation of powers, the judiciary neither creates the laws (the role of Congress) nor enforces the laws (the role of the President and executive branch department and agencies).[16] This structure ensures that courts are independent entities, tasked with fairly and impartially interpreting and applying laws to resolve disputes. The independence of the federal judiciary is grounded in the US Constitution, which requires federal judges to be appointed for life.

In practice, this means that when a law enforcement agency (part of the executive branch) seeks a warrant to obtain information held by a technology company, that warrant application is reviewed by an independent judge (part of the judiciary branch).

LEGISLATIVE BRANCH
Congress—Creates Laws

Congress creates laws that specify the circumstances in which law enforcement agencies may seek a warrant and the standards for issuing a warrant; these laws supplement Constitutional requirements

EXECUTIVE BRANCH
President—Enforces Laws

Law enforcement agencies are part of the executive branch; they must apply to courts to seek a warrant and must meet requirements imposed by both statutory laws (passed by Congress) and by the Constitution

JUDICIAL BRANCH
Courts—Interpret Laws

Courts issue warrants; they do so only when a law enforcement agency applies for a warrant and meets the requirements imposed by both statutory laws (passed by Congress) and by the Constitution

THE CLOUD ACT HAS TWO PARTS

PART 1

Clarifying that orders under the existing ECPA framework reach data regardless of where it is stored

PART 2

Creating a new framework for government-to-government agreements on cross-border law enforcement requests

The CLOUD Act: A Targeted Amendment to US Law

The CLOUD Act did not create a new legal framework for law enforcement agencies to obtain information held by technology companies. Instead, it made targeted amendments to the longstanding legal framework established by the Electronic Communications Privacy Act (ECPA).

Electronic Communications Privacy Act (ECPA): Enacted in 1986, ECPA was designed to protect the privacy of electronic communications such as emails, including by limiting the circumstances in which law enforcement agencies could seek electronic communications from technology companies.[17] ECPA established the legal framework setting out requirements that law enforcement agencies must meet to seek information from technology companies.[18]

Clarifying Lawful Overseas Use of Data (CLOUD) Act: Enacted in 2018, the CLOUD Act amended ECPA to clarify that the location in which data is stored is not the deciding factor in whether a court may issue an ECPA warrant.[19] As a result, the CLOUD Act did not create an entirely new legal structure under which data can be obtained by US law enforcement agencies—but instead clarified how ECPA's legal framework applies in a specific scenario, when the data sought is not stored in the United States.[20] In practice, orders governed by the CLOUD Act are still issued under the longstanding legal framework established by ECPA—and are often referred to as simply "ECPA warrants" or "ECPA orders." The CLOUD Act also expressly preserves the ability of providers to bring common law "comity challenges" if an order conflicts with a foreign country's law.[21]

What Are CLOUD Act Agreements?

The second part of the CLOUD Act creates a framework for new government-to-government agreements to govern cross-border access to data held by technology providers. Currently, law enforcement agencies in one country seeking evidence stored in another country use the Mutual Legal Assistance Treaty (MLAT) process. The CLOUD Act sets out a new framework, with specific requirements a country must meet before the United States may enter into a CLOUD Act agreement. These include showing the country's domestic law affords robust substantive and procedural protections for privacy and civil liberties, based on a series of factors set out in the statute.[22] In addition, if a US warrant conflicts with the law of a foreign country that has entered into a CLOUD Act agreement, the Act provides an additional mechanism for technology companies to challenge the warrant in court.[23]

In October 2019, the United States and United Kingdom entered into the first CLOUD Act agreement.[24] In 2021, the United States and Australia entered into the second CLOUD Act agreement.[25] The United States has also begun formal negotiations with both the European Commission and Canada, to further facilitate access to electronic evidence in criminal investigations.[26]

Endnotes

[1] The CLOUD Act was passed as part of the Consolidated Appropriations Act, 2018, Pub. L. No. 115-141 (March 23, 2018), https://www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf. *See* Division V, CLOUD Act (amending the Electronic Communications Privacy Act, 18 U.S.C. 2701 et seq).

[2] *Id.*

[3] *See* 18 U.S.C. 2713 (added to ECPA by Sec. 103 of the CLOUD Act).

[4] *See* 18 U.S.C. 2523.

[5] *See* 18 U.S.C. 2703(a) (requiring warrants to be issued under the criminal procedures of federal or state courts); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

[6] *See* Seeking Enterprise Customer Data Held by Cloud Service Providers, U.S. Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division (December 2017), https://www.justice.gov/criminal-ccips/file/1017511/download.

[7] Without prior court approval, a government agency may only obtain a limited set of information with a subpoena, which can seek seven specific types of data identified in the statute, including a subscriber's name, address, and billing information. 18 U.S.C. 2703(c)(2). A court order issued on a lesser showing than a warrant may be obtained to seek non-content data, such as transactional data; this requires a showing that articulable facts show reasonable grounds to believe the information sought is relevant and material to an ongoing criminal investigation. 18 U.S.C. 2703(d).

[8] *See* 18 U.S.C. 2703 note (2018) (Rule of Construction).

[9] 18 U.S.C. 2703 note (2018) (Rule of Construction).

[10] *See* Restatement (Third) of Foreign Relations Law § 442. Other factors to be considered include (1) the importance to the investigation or litigation of the documents or information requested; (2) the extent to which noncompliance with the request would undermine important interests of the United States, and (3) the extent to which compliance with the request would undermine important interests of the state where the information is located.

[11] *See* 18 U.S.C. 2702(a)-(b) (prohibiting ECS and RCS providers from disclosing digital content except in nine specific circumstances, including pursuant to a warrant, with the consent of the recipient, and as needed to render the service).

[12] The CLOUD Act amends ECPA; orders under these authorities can reach electronic communications service providers ("ECS providers") and remote computing service providers ("RCS providers"). *See* 18 U.S.C. 2511(15) (defining ECS providers); 18 U.S.C. 2711(2) (defining RCS providers).

[13] *See* 18 U.S.C. 2713 (stating that orders may reach information within a provider's "possession, custody or control"). *See* 18 U.S.C. 2713.

[14] A company is subject to jurisdiction in the US if it has "minimum contacts" with the United States, such as when a foreign business "purposefully avails" itself of the privilege of conducting business in the United States by serving US customers.

[15] *See* United States Constitution, Article III.

[16] *See, e.g.*, Administrative Office of the US Courts, Understanding the Federal Courts, https://www.uscourts.gov/sites/default/files/understanding-federal-courts.pdf.

[17] Pub. L. No. 99-508 (1986), https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf.

[18] *See, e.g.*, House Report No. 99-647 (1986), https://www.justice.gov/sites/default/files/jmd/legacy/2013/10/16/houserept-99-647-1986.pdf; Senate Report No. 99-541 (1986), https://www.justice.gov/sites/default/files/jmd/legacy/2014/08/10/senaterept-99-541-1986.pdf.

[19] Pub. L. No. 115-141 (March 23, 2018), https://www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf. *See* Division V, CLOUD Act (amending the Electronic Communications Privacy Act, 18 U.S.C. 2701 et seq.).

[20] *See* 18 U.S.C. 2713 (added to ECPA by CLOUD Act).

[21] 18 U.S.C. 2703 note (2018) (Rule of Construction).

[22] 18 U.S.C. 2523(b)(1).

[23] 18 U.S.C. 2703(h)(2)(A).

[24] *See US and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online*, Department of Justice, October 3, 2019, https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.

[25] *See* Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime (December 15, 2021).

[26] *See* Justice Department and European Commission Announces Resumption of U.S. and EU Negotiations on Electronic Evidence in Criminal Investigations (March 3, 2023) and United States and Canada Welcome Negotiations of a CLOUD Act Agreement (March 22, 2022).