wiley

ALERT

The CLOUD Act Data Access Agreement – 10 Things That U.S. Telecommunications Companies Need to Know Now

October 27, 2022

Most of the world's popular telecommunications services, like social media platforms and message services, operate within the United States, but many operate overseas as well. Law enforcement in the United States and investigators in foreign countries increasingly seek access to electronic communications such as emails or text messages during the course of their investigations that are stored either in data centers in the United States or overseas. As a result, electronic communications that may be evidence of a crime are often not stored in the same country where the crime occurred. This frequently led U.S. and foreign investigators to seek evidence from technology companies that stored data outside their territorial jurisdictions.

U.S. law historically prohibited telecommunications companies operating within U.S. jurisdiction from sharing certain data in response to requests made directly by a foreign government. While mutual legal assistance treaties (MLAT) did provide a mechanism for allowing government-to-government requests for electronic communications data, the MLAT process was notoriously slow, often taking months to complete, while hampering critical investigations in the United States and abroad.

The Clarifying Lawful Overseas User of Data (CLOUD) Act was enacted by Congress to govern cross-border access to electronic communications held by private companies.[1] The CLOUD Act has two major components:

Authors

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
jfbrown@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Privacy, Cyber & Data Governance

1) Technology companies can be compelled to disclose data held overseas. The CLOUD Act addresses the U.S. government's ability to compel telecommunications companies to disclose the contents of electronic communications stored on the companies' servers and data centers overseas. The Stored Communications Act (SCA)[2] mandates that certain telecommunications companies disclose the contents of electronic communications if served with a warrant based on probable cause that the communications are evidence of a crime. The CLOUD Act amended the SCA to require tech companies to provide data in their possession, custody, or control regardless of whether the data was located in the United States.[3]

2) Foreign governments can reciprocally gain access to data from U.S. telecommunications companies that is evidence of a crime. The CLOUD Act addresses the reciprocal issue of foreign governments' ability to access data in the United States as part of their investigation and prosecution of crime. Prior to the CLOUD Act, foreign governments seeking data in the United States were required to request the assistance of the U.S. government through either MLAT requests or letters rogatory. Both require judicial review before disclosure to a foreign government or agency can be authorized. Both the U.S. and foreign officials criticized the MLAT/letters rogatory process as slow, inefficient, and unable to keep up with the increasing volume of data requests in the digital era.[4]

CLOUD Act Modernizes Cross-Border Data Sharing in Serious Criminal Investigations

The CLOUD Act attempted to modernize cross-border data sharing in serious criminal investigations by clarifying U.S. law and by authorizing a new executive agreement so that foreign governments or foreign agencies could seek data directly from U.S. telecommunications companies without individualized review by the U.S. government. Agreements authorized by the CLOUD Act remove legal restrictions on certain countries' ability to seek data directly from U.S. service providers in cases involving "serious crimes," not targeting U.S persons, when the United States has determined that the foreign country meets certain requirements such as adequately protecting privacy and civil liberties.5

The CLOUD Act speeds up access to electronic information held by U.S.-based global providers that is critical to foreign partners' investigations of serious crime (ranging from terrorism to violent crime to sexual exploitation of children and cybercrime). The CLOUD Act is supposed to represent 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 and changes in the way global tech companies store their data.

U.S.-U.K. Data Access Agreement Entered Into Force on October 3, 2022

In 2019, the United States and the United Kingdom (U.K.) signed an agreement to access electronic data for the purpose of countering serious crime (which is known as the Data Access Agreement (DAA)).[6] For the United States, the agreement was authorized by the CLOUD Act. For the U.K., however, Parliamentary approval was necessary. Both countries see the agreement as starting a new era of cooperation between the U.S. and the U.K. supporting a renewed commitment to tackling the threat of serious crime.

The U.S.-U.K. DAA allows U.S. and U.K. law enforcement to directly request data held by telecommunications providers in the other party's jurisdiction to prevent, detect, investigate, and prosecute serious crime. This includes subscriber information as well as content. The DAA is expected to transform the ability of U.S. and U. K. law enforcement to promptly and efficiently access data that is vital to keeping people safe. The U.K.'s Crime (Overseas Production Orders) Act of 2019 grants law enforcement agencies and prosecuting authorities the power to apply for and obtain electronic evidence directly from service providers for criminal investigations and prosecutions but only when under an international cooperation arrangement.

Ten Things U.S. Telecommunications Companies Need to Do as the U.K. Starts to Issue Overseas Production Orders to the United States

As the CLOUD Act with the U.K. goes into force, U.S. companies should consider the following 10 issues as they prepare to receive legal process directly from the U.K.:

1. **U.S. telecommunications companies should evaluate the legal sufficiency of the orders they receive from the U.K**. U.S. tech companies that receive legal process directly from the U.K. should review the legal sufficiency of the orders they receive. The DAA only applies to "serious crime" which is defined as one that could result in a maximum possible term of at least three years and must be for "covered data," which means: the content of an electronic or wire communication; computer data stored or processed for a user; traffic data or metadata pertaining to an electronic or wire communication or the storage or processing of computer data for a user. The data must be held or processed by the telecommunications service provider.
2. **Is there a written certification that the Order is lawful and complies with the DAA, including the U. K.'s substantive requirements?** An order under the DAA must include a written certification by the Issuing Party's Designated Authority that the order is lawful and complies with the DAA, including the Issuing Party's substantive standards for orders subject to the Agreement.
3. **Are targeted accounts described with specificity?** Orders under the DAA must be targeted at specific accounts and must identify as the object of the order a specific person, account, address, or personal device, or any other specific identifier.
4. **Did the U.K. notify the tech company that "it invokes th[e] Agreement with respect to the Order"?** The Issuing Party's Designated Authority must notify the covered provider that it invokes the DAA with respect to the order.
5. **Are orders for the interception of wire or electronic communications for a fixed or limited duration and not longer than is reasonably necessary to accomplish the approved purposes of the Order?** Orders subject to the DAA for the interception of wire or electronic communications, and any extension thereof, must be for a fixed, limited duration and may not last longer than is reasonably necessary to accomplish the approved purposes of the order. Additionally, the order can only be issued if the same information could not reasonably be obtained by another less intrusive method.
6. **Does the company want to challenge the U.K. Order? Does the company have a reasonable belief that the DAA may not be invoked?** A U.S. provider can raise these objections to the U.K.

designated authority (the U.K. Secretary of State). If the objections are not addressed, the provider may raise objections with the U.S. Department of Justice.

7. **Does the U.K. Order target U.S. persons?** The DAA does not permit the targeting of U.S. persons. The U.K. cannot request "covered data" on a U.S. person or on a person located in the United States.
8. **Does the U.K. Order impinge on freedom of speech?** The DAA may not be used to infringe on freedom of speech or for disadvantaging persons based on their race, sex, sexual orientation, religion, ethnic origin, or political opinions.
9. **Comply with any non-disclosure provisions.** The CLOUD Act, however, does not restrict companies from publishing data, for instance on the number of requests they receive from the U.K. for transparency reports.
10. **Decryption is not obligated.** Electronic data must be produced or accessible in a visible or legible form. The CLOUD Act is "encryption neutral." It does not create any new authority for law enforcement to compel service providers to decrypt communications nor does it prevent service providers from assisting in such decryption or prevent countries from addressing decryption requirements in their own domestic laws.

The DAA with the U.K. is the first CLOUD Act agreement to go into force. The United States signed a similar agreement with Australia on December 15, 2021 that is expected to go into force by the end of the year.[7] The United States has also announced that it is in formal negotiations for additional bilateral agreements under the CLOUD Act with Canada[8] as well as with the European Union[9] on electronic evidence sharing.

U.S. communications service providers and tech companies need to be ready to receive legal process seeking subscriber information or content directly from countries that have CLOUD Act agreements with the United States, starting with U.K. agencies. Each CLOUD Act agreement is separately negotiated and terms may vary. Companies need to understand the obligations they have under each separate agreement in order to properly comply with its terms. Advance planning for when CLOUD Act requests are received will help companies provide responsive electronic data in a timely fashion and avoid data production errors.

Wiley has a long history of assisting telecommunications companies with responding to legal requests and providing assistance to law enforcement. Companies would be wise to start preparing for these new legal requirements before legal process from CLOUD Act agreements is served upon them.

---

[1] Clarifying Lawful Overseas User of Data (CLOUD Act), Pub. L. 115–141, div. V, § 105(a), Mar. 23, 2018, 132 Stat. 1217; 18 U.S.C. § 2523.
https://www.justice.gov/dag/page/file/1152896/download

[2] 18 U.S.C. § 2701, *et seq.*

[3] *Justice Department Announces Publication of White Paper on the CLOUD Act*, U.S. Department of Justice, April 10, 2019.

[4] *Id.*

[5] *Promoting Public Safety, Privacy, and the Rule of Law Around the World: the Purpose and Impact of the CLOUD Act*, U.S. Department of Justice, White Paper April 2019.

[6] Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, with side letters concerning the implementation and application of the Agreement (DAA). https://www.justice.gov/dag/page/file/1231381/download

[7] *See* Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purposes of Countering Serious Crime (December 15, 2021). https://www.justice.gov/dag/cloud-act-agreement-between-governments-us-and-australia

[8] *See United States and Canada Welcome Negotiations of a CLOUD Act Agreement*, U.S. Department of Justice, Office of Public Affairs (March 22, 2022). https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement

[9] *See Joint US-EU Statement on Electronic Evidence Sharing Negotiations*, U.S. Department of Justice, Office of Public Affairs (September 26, 2019). https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations