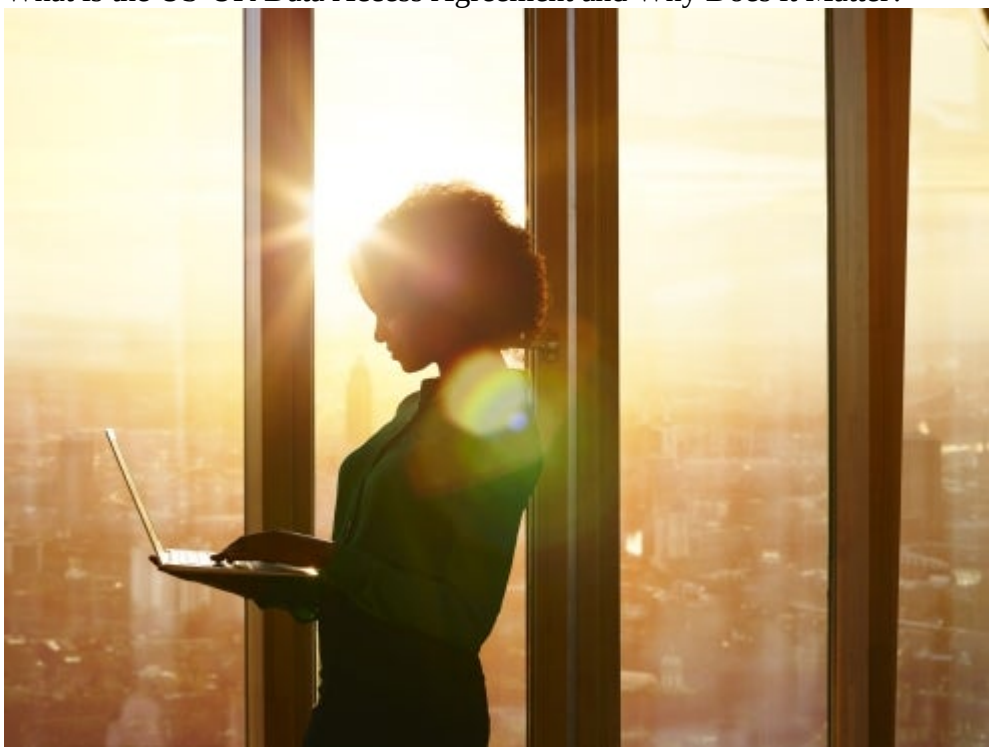
Updates
November 21, 2022
What is the US-UK Data Access Agreement and Why Does it Matter?



This is the second in a series of updates addressing the bilateral data access agreement[1] (Data Access Agreement or agreement) between the United States and the United Kingdom under the Clarifying Lawful Overseas Use of Data Act (CLOUD Act).

The agreement, which entered into force on October 3, 2022, is designed to facilitate cross-border criminal investigations involving communications data. This Update focuses on what the Agreement says and the processes it establishes for service of process.

What is the purpose of the agreement? In short, this framework is designed to overcome restrictions in U.S. law that otherwise prohibit U.S.-based communications providers from complying with certain requests from U.K. authorities who conduct criminal investigations. Specifically, the Stored Communications Act (SCA) prohibits U.S. providers of electronic communication services (ECS) and remote computing services (RCS) from disclosing the contents of communications "to any other person or entity," including foreign governmental entities. The Wiretap Act similarly prohibits providers from intercepting the contents of communications without consent from one of the parties to that communication. While the Stored Communications Act (SCA) and Wiretap Act provide mechanisms for U.S. governmental entities to compel U.S.-based providers to disclose or intercept communications content, neither law provides a similar exception for foreign governmental entities. Thus, generally speaking, foreign law enforcement agencies seeking to obtain the contents of communications from U.S. providers must comply with the notoriously lengthy and cumbersome Mutual Legal Assistance Treaty (MLAT) process, under which U.S. prosecutors obtain legal process on their behalf.

What does the agreement do? The Data Access Agreement implements the CLOUD Act, a statute enacted by Congress in 2018 intended in part to facilitate access by qualifying foreign partners to electronic information held by U.S.-based global providers. Under the Agreement, ECS and RCS providers in the United States can and will begin receiving legal process directly from law enforcement agencies in the United Kingdom.

How does the agreement work? One of the most visible effects of the Data Access Agreement in the U.S. private sector is that authorities in the United Kingdom can serve ECS and RCS providers in the United States with legal process that satisfies *U.K.* legal requirements. The Data Access Agreement permits each country to issue orders to providers in the other that comply with the domestic law of the *issuing* authority and that meet certain requirements, including articulable and credible facts, particularity, legality, and sufficient severity of the conduct under investigation. Orders must relate to a serious crime, defined as an offense that is punishable by a maximum term of imprisonment of at least three years. In addition, orders submitted by U.S authorities must not target U.K. persons or persons located in the United Kingdom and vice versa. Orders that satisfy these requirements can seek disclosure of content and other data from providers located in the other country and may even ask a provider to intercept communications in real time.

Notably, the U.K. legal process that providers receive will not look like U.S. legal process and will operate differently than the warrants, orders, and subpoenas that ECS and RCS providers traditionally receive. For example, in the United States, the Fourth Amendment requires the government to obtain a particularized warrant based on probable cause for each search. The government cannot lawfully use a single warrant to conduct multiple searches. These same restrictions do not apply in the United Kingdom. For example, under Section 17.2 of the Investigatory Powers Act 2016, U.K. authorities can obtain a single warrant instrument that serves as an authorization to conduct several searches over a period of time.

Generally, the agreement is broad enough to cover all the different types of data that communications providers maintain about their users or subscribers. Orders under the agreement must be for "covered data" which means the content of an electronic or wire communication; computer data stored or processed for a user; and traffic data or metadata pertaining to an electronic or wire communication or the storage or processing of computer data for a user. Requests can also be made for subscriber information, meaning information that identifies a subscriber or customer of a provider, including name, address, length and type of service, subscriber number or identity (including assigned network address and device identifiers), telephone connection records, records of session times and durations, and means of payment.

The United States and United Kingdom have each selected certain authorities responsible for the implementation of the agreement. In the United States, the U.S. Department of Justice's Office of International Affairs (OIA) is the designated authority. OIA has created a CLOUD team specifically focused on reviewing and certifying orders, transmitting certified orders to U.K. service providers, and arranging for the return of responsive data. For the United Kingdom, the Investigatory Powers Unit of the Home Office ensures the proper implementation of the agreement.

How might a provider object to legal process under the agreement? A provider that receives an order may raise specific objections when it reasonably believes that the order is not consistent with the agreement. A provider must raise such an objection first to the government that issued the order. If that objection does not resolve the issue, the provider may raise its objections with its own government. For example, if U.S. companies have objections, they should generally raise them first to the U.K. Home Office. Upon receipt of objections, the U.K. Home Office will respond. If the objections are not resolved, the U.S. company can raise such objections to OIA.

As a result of the agreement and these new objection procedures, covered providers in the United States will need to understand whether legal process from the United Kingdom is valid and whether the companies can lawfully comply with such process under U.S. federal law, such as the SCA and the Wiretap Act. And, as part of that analysis, companies will need to make sure that orders are consistent with the agreement itself. For example, the SCA permits a provider to disclose content only "pursuant to an order subject to [the Agreement]." 18 U.S.C. § 2702(b)(9). And Article 4.5 of the agreement states that "Orders subject to this Agreement must be targeted at

specific Accounts and shall identify as the object of the Order a specific person, account, address, or personal device, or any other specific identifier." Thus, if a provider receives an order that does not target a specific person or account, the provider will need to consider whether complying with the order could run afoul of U.S. law. Similarly, Article 4.3 states that "Orders subject to this Agreement may not intentionally target a Receiving-Party Person," which means that an order from the United Kingdom may not target a U.S. person, and vice versa. So, if a U.S.-based provider receives an order that targets a user who the provider determines is a U.S. person, the provider will need to consider how to proceed in a manner consistent with the agreement and U.S. law.

That said, some safeguards are incorporated into the agreement. For example, if authorities in the United Kingdom receive data under the agreement as part of an investigation into an offense that would violate the First Amendment of the U.S. Constitution such as those involving news gathering and publication or public protest, the agreement prohibits the U.K. authority from using this data as evidence without permission from the United States.

As the agreement is barely a month old, many of its nuances remain unexplored. Businesses that may be affected by the agreement should consult with knowledgeable counsel. Perkins Coie's experienced team advises and routinely represents platforms on such matters.

The first post, which provides an overview of the CLOUD Act, the agreement, and their likely effects, can be found here. The remaining questions to be explored in this series include the following:

- How might the agreement affect companies' obligations under European data protection law?
- How does the agreement compare to other existing cross-border paradigms?

Endnote

[1] Formally known as the 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.

This Update is the second in a series.

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law Data Security Counseling and Breach Response Communications

Related insights

Update

Two Tools for Trump To Dismantle Biden-Era Rules: the Regulatory Freeze and the Congressional Review Act

Update

The FY 2025 National Defense Authorization Act: What’s New for Defense Contractors