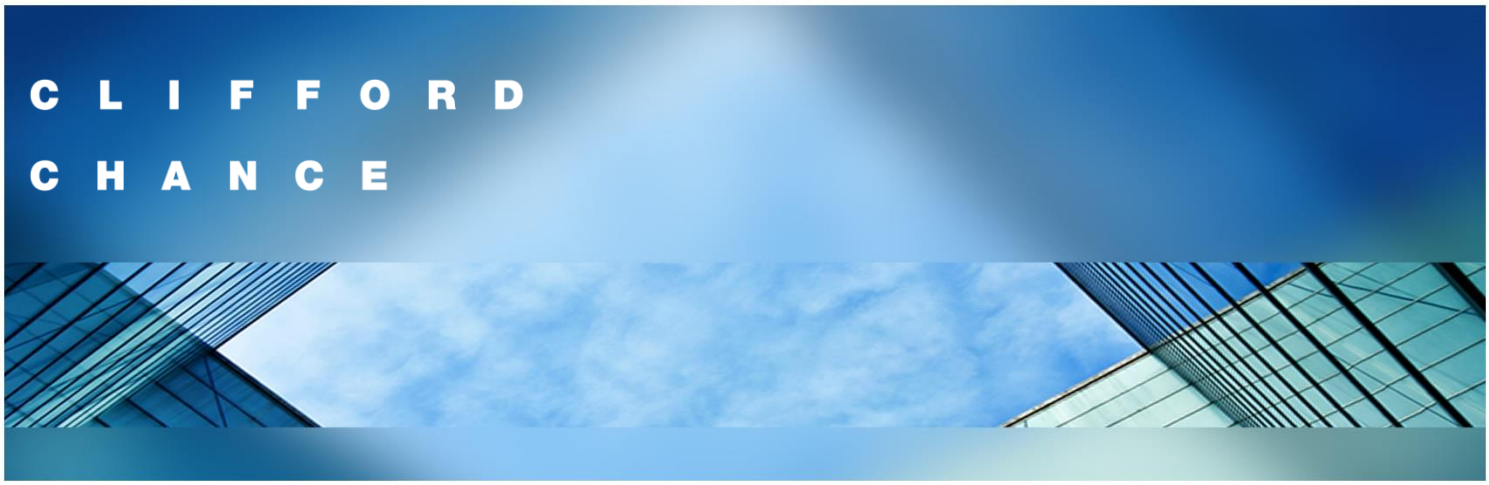

CONGRESS AUTHORIZES THE SEIZURE OF RECORDS STORED OVERSEAS WITH THE CLOUD ACT – BEATING THE SUPREME COURT TO THE PUNCH

The U.S. government now has expanded powers to demand the disclosure of electronic data regardless of where that data is stored under a new federal statute that authorizes the U.S. government to seize data stored overseas. The statute also eventually will allow foreign governments to compel disclosure from companies in the United States.

On March 23, 2018, President Trump signed into law an omnibus spending bill, which included the Clarifying Lawful Overseas Use of Data Act (the "CLOUD Act"). The CLOUD Act amends the Stored Communications Act of 1986 ("SCA") to explicitly authorize U.S. law enforcement agencies to obtain data stored outside the United States from data storage providers through a domestic warrant or court order. While the law exposes foreign-stored records to seizure by U.S. authorities, it also provides a mechanism to challenge that seizure in U.S. courts. The law thus resolves the issue at the core of *United States v. Microsoft*, which is currently pending before the U.S. Supreme Court—at least for future warrants and disclosure orders issued pursuant to the SCA.

Background – *United States v. Microsoft*

Enacted more than thirty years ago, the SCA protects electronic data from unauthorized access, while allowing the U.S. government to require disclosure of such information pursuant to a warrant or court order. Because the SCA did not expressly state that it has extraterritorial reach, Microsoft challenged the U.S. government's attempt to obtain data stored overseas, culminating in *United States v. Microsoft*, which is currently before the U.S. Supreme Court.

As we explained in our previous client alert, the *Microsoft* case centers on whether the SCA (prior to amendment) authorized the U.S. Department of Justice ("DOJ") to demand a customer's e-mails that were stored on Microsoft servers in Ireland, in connection with a drug prosecution. The case raised competing concerns, pitting the possibility of foreign relations disputes over perceived U.S. law enforcement overreach against the potential for bad actors to exploit decentralized data storage and avoid the disclosure of their data to law enforcement.

Key issues

- The CLOUD Act explicitly authorizes U.S. law enforcement agencies to obtain data stored outside the United States from data storage providers through a domestic warrant or court order.
- In addition to expanding the U.S. government's reach over electronic data, the CLOUD Act lays the groundwork for expanding the ability of foreign governments to compel disclosure of data stored in the United States.
- The CLOUD Act affects all companies that engage in cross-border data storage.
- Companies should evaluate their cloud storage practices in view of the new legislation, and should implement policies and procedures to evaluate and respond to both U.S. and foreign requests.

Microsoft argued that the SCA does not authorize the U.S. government to compel production of data stored in foreign countries, since the statute did not apply extraterritorially. DOJ countered that the question of extraterritoriality was beside the point because Microsoft's disclosure would involve primarily domestic conduct—the production of evidence by an entity located in the United States as part of a U.S. criminal investigation.

During oral argument on February 27, 2018, several justices stated that they were aware of the pending new legislation and signaled that the issue may be more appropriately resolved by Congress than by the Court.

The CLOUD Act

The CLOUD Act was introduced as bicameral legislation prior to oral argument in *Microsoft*. Senator Orrin Hatch, the bill's sponsor in the Senate, attended the *Microsoft* oral argument and immediately published a statement, highlighting that the "Justices continually referred to the importance of action from Congress."

Amending the SCA to expressly authorize law enforcement agencies to obtain data stored outside the United States, the CLOUD Act requires providers of electronic communication or remote computing service to preserve, backup, or disclose, pursuant to a warrant or a court order, electronic data that is within the "provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."[1]

The CLOUD Act makes clear that, going forward, a warrant such as that issued in the *Microsoft* case would be authorized, albeit subject to challenge under the safeguards in the CLOUD Act described below. On March 30, the U.S. government filed a motion with the Supreme Court to vacate the judgment of the Second Circuit, on the basis that it has obtained a new warrant under the CLOUD Act to seize the data under Microsoft's control. While not conceding its arguments before the Supreme Court, the U.S. government argues that the CLOUD Act and the warrant issued under it render the dispute moot and that vacatur is appropriate to avoid an erroneous opinion that could "'spawn[] legal consequences' in future cases . . . on critical issues involving extraterritoriality and privacy."[2] The Supreme Court will first consider the Government's motion and therefore may not issue an opinion in the *Microsoft* case; nonetheless, if it does, the opinion's impact would be limited to disclosure orders obtained prior to amendment of the SCA.

The CLOUD Act Provides a Mechanism to Challenge Disclosure

Under the CLOUD Act, a data storage service provider can go to court to challenge a U.S. government order requiring disclosure of data that is located in a country with a "qualifying foreign government." The CLOUD Act permits a provider, upon receiving an order to disclose a customer's wire or electronic communication, to file a motion to modify or quash the order. The courts may modify or quash the order only if (i) "the required disclosure would cause the

1 CLOUD Act § 103(a) (to be codified at 18 U.S.C. § 2713).
2 Gov't Mot. To Vacate at 2, *United States v. Microsoft*, No. 17-2 (U.S. Mar. 30, 2018), https://www.supremecourt.gov/DocketPDF/17/17-2/41851/20180330172237829_17-2motUnitedStates.pdf.

provider to violate the laws of a qualifying foreign government;" (ii) "based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed"; and (iii) "the customer or subscriber is not a United States person and does not reside in the United States."[3] In deciding a motion to modify or quash under the CLOUD Act, the court must perform a comity analysis, considering the various interests at stake including those of the U.S. government and the foreign government, the likelihood and nature of penalties that may be imposed on the provider, and the importance to the investigation of the information required to be disclosed.[4]

For data stored in a non-qualifying foreign country (currently all countries, until executive agreements are adopted), traditional means of resisting disclosure appear to remain available, including common law international comity arguments. The CLOUD Act explicitly states that "[t]he right to move to quash [as prescribed in the CLOUD Act] is without prejudice to any other grounds to move to quash or defenses thereto, but it shall be the sole basis for moving to quash on the grounds of a conflict of law related to a qualifying foreign government."[5]

A New Framework for Law Enforcement to Access Cross-Border Data

In addition to expanding the U.S. government's reach over electronic data, the CLOUD Act lays the groundwork for expanding the ability of foreign governments to compel disclosure of data stored in the United States by establishing a new framework for the United States and foreign governments to enter into executive agreements to facilitate the cross-border transfer of data for law enforcement purposes.

Even before enactment of the CLOUD Act, the United Kingdom and the United States had begun negotiating an agreement to streamline the process for the transfer of data between the two countries for law enforcement purposes, driven by the burdensome nature of the pre-existing process. Indeed, the United Kingdom filed an *amicus curiae* brief in the *Microsoft* case, arguing that the process for seeking electronic communications from the United States or other countries through Mutual Legal Assistance Treaty ("MLAT") requests is cumbersome and slow and can inhibit effective law enforcement investigations.

Under the new framework, the CLOUD Act grants privileged status for "qualifying foreign government[s]." A foreign government may become "qualifying" by entering into an executive agreement with the United States, which must be approved by the U.S. Attorney General and the U.S. Secretary of State.[6]

The CLOUD Act permits data storage service providers to disclose customer data in response to a court order from a qualifying foreign government if the provider is required to make the disclosure under the foreign government's law and the order is issued in connection with the investigation of a serious crime.[7] Pursuant to an

---

3 CLOUD Act § 103(b) (to be codified at 18 U.S.C. § 2703(h)(2)(B)).
4 CLOUD Act § 103(b) (to be codified at 18 U.S.C. § 2703(h)(3)).
5 CLOUD Act § 103(b) (to be codified at 18 U.S.C. § 2703(h)(2)(ii)).
6 CLOUD Act § 103(b) (to be codified at 18 U.S.C. § 2703(h)(1)(A)(i)); CLOUD Act § 105(a) (to be codified at 18 U.S.C. § 2523(b)).
7 CLOUD Act § 104(2)(A)(i) (to be codified at 18 U.S.C. § 2702(b)(9)); CLOUD Act § 104(2)(A)(ii) (to be codified at 18 U.S.C. § 2702(b)(9)); CLOUD Act § 105(a) (to be codified at 18 U.S.C. § 2523(b)(3)(D)(i), (iii)).

order from a qualifying foreign government, service providers may also intercept or disclose the contents of a wire or electronic communication, through the CLOUD Act's amendment of the Wiretap Act, 18 U.S.C. § 2511.[8] When a data provider complies with an order from a qualifying foreign government, the CLOUD Act immunizes the service provider from civil causes of action for providing the data to that government.[9]

The CLOUD Act incorporates numerous restrictions intended to ensure that foreign governments do not abuse access to data stored by U.S. service providers or use the data for malicious purposes. Specifically, the legislation requires "the Attorney General, with the concurrence of the Secretary of State" to certify in writing to Congress that "the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties," and that the foreign government adopts procedures to maintain the security of the data and limit its use to the criminal investigation.[10] In addition, the CLOUD Act requires an order issued by a foreign government to (i) identify a specific person, account, address, or personal device as the object of the order;[11] (ii) comply with the foreign country's domestic law;[12] (iii) be subject to review by a court, judge, magistrate, or other independent authority in the foreign country;[13] and (iv) not serve as a means of providing communication of a U.S. person to the U.S. government, except under limited circumstances.[14] And the qualifying foreign government must provide reciprocal rights of access to service providers responding to U.S. government requests for data even if its domestic law would otherwise prohibit disclosure.[15]

The Future of Data Privacy

The CLOUD Act affects all companies that engage in cross-border data storage. Many technology companies, including Microsoft, have applauded the legislation for providing clearer rules and procedures for data disclosure, particularly in situations in which the company is potentially subject to conflicting laws in multiple jurisdictions.

Nonetheless, litigation is likely to ensue regarding attempts to resist orders submitted pursuant to the CLOUD Act. As evidenced by the international interest in the *Microsoft* case, many foreign governments view electronic data collection by U.S. government agencies as potentially conflicting with their domestic interests. The European Community and other countries who filed *amici curiae* in *Microsoft* argued that an extraterritorial application of U.S. law would likely create inter-jurisdictional conflict. Particularly in the near term, before agreements with "qualifying" foreign governments are negotiated, companies grappling with incoming requests will have to determine whether and how to challenge a disclosure order without running afoul of either U.S. or foreign law.

---

8 CLOUD Act § 104(1)(A) (to be codified at 18 U.S.C. § 2511(2)(j)).
9 CLOUD Act § 104(3)(B)(i), (ii) (to be codified at 18 U.S.C. §§ 3124(d), 3124(e)).
10 CLOUD Act § 105(a) (to be codified at 18 U.S.C. §§ 2523(b)(1), 2523(b)(3)(F), 2523(b)(3)(G)).
11 CLOUD Act § 105(a) (to be codified at 18 U.S.C. § 2523(b)(3)(D)(ii)).
12 CLOUD Act § 105(a) (to be codified at 18 U.S.C. § 2523(b)(3)(D)(iii)).
13 CLOUD Act § 105(a) (to be codified at 18 U.S.C. § 2523(b)(3)(D)(v)).
14 CLOUD Act § 105(a) (to be codified at 18 U.S.C. § 2523(b)(3)(H)).
15 CLOUD Act § 105(a) (to be codified at 18 U.S.C. § 2523(b)(3)(I)).

Companies should evaluate their cloud storage practices in view of the new legislation, and should implement policies and procedures to evaluate and respond to both U.S. and foreign requests. Clifford Chance's global network of data and privacy experts is available to assist clients with achieving effective solutions.

CONTACTS

Steve Nickelsburg
Partner

T +1 202 912 5108
E steve.nickelsburg
@cliffordchance.com

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Adam Goldstein
Associate

T +1 202 912 5114
E adam.goldstein
@cliffordchance.com

Alexander Feldman
Associate

T +1 212 878 8042
E alexander.feldman
@cliffordchance.com

Rebecca Hekman
Associate

T +1 202 912 5539
E rebecca.hekman
@cliffordchance.com

Susan Foster
Associate

T +1 202 912 5129
E susan.foster
@cliffordchance.com

Daniel Podair
Associate

T +1 212 878 4989
E daniel.podair
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 2001 K Street NW
Washington, DC, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.