Alert
White Collar Defense & Investigations

Weil

April 19, 2018

# In Wake of CLOUD Act, Supreme Court Agrees that Challenge to Stored Communications Act is Moot

*By Sarah Coyne and Agustina Berro*

On Tuesday, the Supreme Court vacated the Second Circuit's decision in *Microsoft Corp. v. United States* and remanded the case to the appellate court with instructions to direct the District Court for the Southern District of New York to dismiss the case as moot, ending the dispute between the government and Microsoft over whether the Stored Communications Act requires disclosure of electronic communications stored overseas or whether requiring an internet service provider to produce these communications constitutes an impermissible extraterritorial application of the SCA. The order came after both the government and Microsoft sought dismissal, agreeing that the CLOUD Act mooted the case.

The underlying dispute in *Microsoft* arose when U.S. law enforcement officials obtained a warrant pursuant to the SCA for the production of an individual's emails, the content of which was stored on Microsoft's cloud storage servers in Dublin, Ireland. Enacted in 1986, the SCA required that, upon a threshold showing by law enforcement authorities, third-party internet service providers must turn over the electronic communications of their customers, including emails. For years, providers, including Microsoft, had routinely complied with such warrants. However, in response to this warrant, after producing the non-content portion of the requested data (*i.e.*, the metadata), which was stored in the United States, Microsoft moved to quash the remainder of the warrant on the grounds that the content data was located in Ireland, beyond the reach of the U.S. government. Microsoft argued that requiring it to turn over the emails would constitute an extraterritorial application of the SCA despite the fact that—with just a few clicks from inside of its U.S. headquarters—it could easily access and disclose the data in the United States.[1] Although the Magistrate and District Courts ruled in favor of the government, the Second Circuit sided with Microsoft. Having lost in its efforts to obtain the email content that was stored on a server in Ireland, the government petitioned for a rehearing *en banc*, which was narrowly denied by a 4-4 vote.

Despite the absence of a circuit split, the Supreme Court granted *certiorari*, prompting voluminous briefing, including the filing of over 30 *amicus* briefs. During oral argument, the Supreme Court highlighted several areas of concern that had been raised by the parties. Some justices were concerned that physical acts—however minor and computerized—would have to happen in Ireland before the documents could be produced in the United States,

while others seemed troubled by the practical implications of affirming the Second Circuit, noting that nothing would prevent Microsoft from hiding its customers' information beyond the reach of U.S. law enforcement agencies. Several of the justices also expressed concern regarding potential conflicts of law that would expose internet service providers like Microsoft to liability for breaching other countries' privacy laws.

Shortly after the oral argument, Congress somewhat hastily enacted the CLOUD Act, which requires, among other things, that an internet service provider disclose the contents of electronic communications *regardless* of whether the information is located *within or outside* of the United States. The Act establishes a statutory comity framework whereby an internet service provider may move to quash or modify the order requiring disclosure if it believes that (1) the customer whose data is requested is neither a U.S. person nor a U.S. resident, and (2) the required disclosure would create a material risk that the provider would violate the laws of a "qualifying foreign government." CLOUD Act § 103(b).[2] The CLOUD Act also establishes a process for qualifying governments to enter into bi-lateral executive agreements that permit their respective law enforcement agencies, in certain tightly prescribed circumstances, to serve warrants directly on an internet service provider in the partner country, rather than having to obtain the data via a cumbersome mutual legal assistance treaty (MLAT) request.

While many, including both the U.S. government and Microsoft, have praised the CLOUD Act for creating a framework that seeks to balance international cooperation and reciprocal sharing of information against the need to protect an individual's privacy and civil liberties, the Act leaves several open questions. For example, it is unclear how the Act impacts pre-existing mutual legal assistance treaties or whether it conflicts with the E.U.'s General Data Protection Regulation Act, which prohibits disclosure of information unless such disclosure is pursuant to an MLAT. Moreover, the extent to which the statutory comity framework will be applied with any rigor is uncertain. Finally, it remains to be seen whether Microsoft will challenge this warrant, too.

---

[1] *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft*, 855 F.3d 53, 61 (2d Cir. 2017) (noting that the information in question is "easily accessible in the United States at a computer terminal").

[2] The ability to quash a warrant, however, may be somewhat illusory. As the E-Discovery Institute pointed out in its *amicus* brief, when applying the framework set forth in *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522 (1987)—the Supreme Court's seminal decision on cross-border discovery and comity—courts find in favor of discovery (*i.e.*, in favor of violating foreign discovery laws) by a ratio of at least four to one. *See* E-Discovery Institute *Amicus* Br. at 18, *citing* Geoffrey Sant, *Court-Ordered Law Breaking: U.S. Courts Increasingly Order the Violation of Foreign Law*, 81 Brook. L. Rev. 181 (2015). Thus, in practical terms, the CLOUD Act arguably restores the pre-*Microsoft* status quo: internet service providers will have to produce documents regardless of where they are located.

***White Collar Defense & Investigations*** is published by the Litigation Department of Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

For more information about Weil's White Collar Defense & Investigations practice, please contact:

**Editors:**

| | | | |
|---|---|---|---|
| Steven A. Tyrrell (DC) | View Bio | steven.tyrrell@weil.com | +1 202 682 7213 |
| Holly E. Loiseau (DC) | View Bio | holly.loiseau@weil.com | +1 202 682 7144 |
| Adam G. Safwat (DC) | View Bio | adam.safwat@weil.com | +1 202 682 7236 |

**Contributing Authors:**

| | | | |
|---|---|---|---|
| Sarah Coyne (NY) | View Bio | sarah.coyne@weil.com | +1 212 310 8920 |
| Agustina Berro (NY) | View Bio | agustina.berro@weil.com | +1 212 310 8937 |