BRACEWELL

INSIGHTS

CLOUD Act Aims for Clear Skies: Bipartisan CLOUD Act Seeks to Clarify Law Enforcement Access to Overseas Data

February 16, 2018

In October 2017, the Supreme Court granted the Department of Justice's petition to review the Second Circuit's decision that limits the reach of warrants issued under the Stored Communications Act ("SCA").[1] Specifically, the Court will determine whether the SCA can be used to obtain information stored in data centers abroad. Oral argument has been scheduled for later this month. This case stemmed from a 2013 warrant for Microsoft data held in Irish data centers. Microsoft moved to quash the warrant and refused to turn over the requested information, arguing that the SCA warrant forced the company to choose between complying with U.S. law enforcement and violating privacy laws in other countries that prohibit such disclosures. Instead, Microsoft urged the government to pursue bilateral law enforcement and diplomatic channels in order to obtain the requested information. Initially, the U.S. District Court ordered Microsoft to comply with the warrant, but Microsoft was successful in quashing the warrant in its appeal to the U.S. Court of Appeals for the Second Circuit. The Second Circuit held that Congress did not intend to extend the SCA's warrant provision extraterritorially, and after the Second Circuit denied rehearing *en banc*, the government appealed to the Supreme Court. Similar cases are being litigated around the country, and courts have come to different conclusions.[2]

Many other multinational data center operators and a bipartisan group of members of Congress filed amicus briefs in support of Microsoft. In the Congressional amicus brief,[3] Senators Hatch, Coons, Collins and Jeffries, along with Representative Darrell Issa, argue that the Court should not depart from the presumption against extraterritoriality, a principle in statutory interpretation that provides that, unless Congress explicitly says otherwise, U.S. laws do not extend past the country's borders. The brief further argues that "Congress, not this court, is the appropriate branch to address the solicitor general's concerns — through affirmative legislation." In an effort to settle the issue and provide the legislation foreshadowed by the Congressional amicus brief, on February 6, 2018, a bipartisan group of senators, including Senators Graham, Hatch, Coons, and Whitehouse, proposed the Clarifying Lawful Overseas Use of Data ("CLOUD") Act of 2018.[4] Representative Collins introduced a companion bill in the House of Representatives the same day. The CLOUD Act was negotiated with, and draws support from, technology companies and U.S. law enforcement, including the Department of Justice.

The CLOUD Act may provide benefits to the litigants in the Microsoft case and similar disputes.[5] It appeals to U.S. law enforcement by clarifying that all data that is in the "possession, custody, or control" of American "communications-service" (data) providers, wherever that data is

stored, is reachable by SCA warrants, subject to principles of international comity.[6] In addition, the CLOUD Act would require participating countries to remove legal restrictions that prevent compliance with data requests from U.S. law enforcement.[7] American service providers gain a clear process for following and challenging government requests for data stored abroad, such as the statutory right to challenge warrants for data regarding foreign nationals based on comity concerns, as well as a process by which to notify certain foreign governments of requests regarding foreign nationals. The CLOUD Act also contains potential benefits for foreign governments seeking to protect the information of their citizens, and also provides a mechanism for assistance from U.S. companies during foreign law enforcement investigations. Under the Act, foreign governments could enter into bilateral agreements with the U.S. government, and countries that do so would then be permitted to challenge U.S. law enforcement requests deemed inappropriate. In addition, the bill permits foreign governments to request content regarding foreign nationals directly from American providers under executive agreements, if the country meets a set of requirements. These requirements include: (1) robust substantive and procedural protections for privacy and civil liberties and (2) appropriate procedures to minimize the acquisition, retention, and dissemination of information.

After being introduced, the Senate's CLOUD Act was referred to the Senate Committee on the Judiciary for review. Its companion in the House was referred to the House Committee on Rules and the House Committee on the Judiciary. If it becomes law, the CLOUD Act would become the second recent change to complex data gathering processes in criminal investigations. It will join the Department of Justice's Computer Crime and Intellectual Property Section, Criminal Division December 2017 guidance advising prosecutors seeking enterprise customer data stored "in the cloud" to attempt to collect responsive information from the enterprise first, instead of serving information requests directly on the enterprise's cloud data service provider. For both data storage providers and those who rely on cloud data services for email and other information storage, these developments are a good reminder to make sure the right personnel and technology are in place, to responsibly collect data and provide timely and complete responses to direct requests from the government.

---

[1] The SCA was enacted as part of the Electronic Communications Privacy Act of 1986. It addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by internet service providers. The full text of the SCA is available ***here.***

[2] For example, in In re Search Warrant No. 16-960-M-01 to Google, a magistrate judge ordered that Google comply with a search warrant to produce information stored overseas. Google has put its appeal on hold pending the outcome of the Microsoft case.

[3] The amicus brief is available ***here***.

[4] The CLOUD Act is available ***here***.

[6] In fact, U.S. and British law enforcement have come out forcefully in support of the bill. In a February 15 op-ed in The New York Times, Thomas Bossert, the assistant to the president for

homeland security and counterterrorism, and Paddy McGuinness, the deputy national security adviser for Britain, argue that the CLOUD Act would "preserve law and order, advance the United States' leadership in cybersecurity, ease restrictions on American businesses and enhance privacy standards globally."

[5] Consumer groups, however, such as the Electronic Frontier Foundation, argue that the CLOUD Act "privileges law enforcement at the expense of people's privacy." Their post on the CLOUD Act is available ***here***.

[7] The proposed bill has received early support from the U.K. https://www.gov.uk/government/news/pm-call-with-president-trump-6-february-2018