New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 259—NO. 107
TUESDAY, JUNE 5, 2018

FEDERAL E-DISCOVERY

CLOUD Act Governs Warrants for Data Stored Outside U.S.

By **Christopher Boehning**

And **Daniel J. Toal**

SHUTTERSTOCK

Microsoft's four-year legal battle over the U.S. government's ability to subpoena customer email stored outside of the United States ended abruptly thanks to the passage of new legislation directly governing the subject matter. On March 23, 2018, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) was signed into law as part of the omnibus spending bill. Only three weeks earlier, Microsoft and the United States each appeared before the U.S. Supreme Court to present argument on the appropriate reach of the government in warrants issued under the Stored Communications Act (SCA). After the passage of the CLOUD Act, the court vacated the prior lower court decisions and directed the district court to dismiss the case as moot. While the CLOUD Act provides clarity as to the permissible reach of the U.S. government, it raises issues of potential conflicts with the laws of other countries, especially as data privacy laws are being strengthened in Europe and elsewhere.

'Microsoft" Case

The *Microsoft* case arose when the U.S. government obtained a warrant under Section 2703 of the SCA for email content and information from a Microsoft Network (msn.com) email account. Microsoft had moved to quash the warrant to the extent that it sought information stored on servers outside the United States, specifically in Ireland. The legal question presented was whether a probable-cause-based warrant issued by a magistrate judge under the SCA reaches digitally-stored materials within a service provider's control, but stored abroad. The U.S. Court of Appeals for the Second Circuit, reversing the district court, held that the SCA did not require service providers to produce email content stored outside the U.S. The Supreme Court granted certiorari and heard argument on February 27, 2018.

Soon thereafter, the CLOUD Act, which directly addressed the question implicated in the *Microsoft* case concerning the extraterritorial reach of the SCA, became law. The CLOUD Act amends the SCA, expressly requiring email service providers to preserve, back up, and disclose to U.S. law

CHRISTOPHER BOEHNING *and* DANIEL J. TOAL *are litigation partners at Paul, Weiss, Rifkind, Wharton & Garrison.* ROSS M. GOTLER, *e-discovery counsel,* LIDIA M. KEKIS, *e-discovery attorney, and* REBECCA L. OREL, *associate, assisted in the preparation of this article.*

enforcement electronic data responsive to a warrant issued under the SCA within their "possession, custody, or control," even when that data is located outside the United States. Microsoft, despite its position in the long-running dispute, supported the passage of the CLOUD Act along with other tech giants such as Google and Apple, taking the position that new legislation was needed to update the relevant law, especially with respect to cloud service providers. The U.S. Department of Justice subsequently obtained a new warrant under Section 2703 of the now-amended SCA for the email account at issue in the *Microsoft* case. It then asked the court to dismiss the case as moot; Microsoft did not object.

Challenging a Data Warrant

In clarifying the ability of U.S. law enforcement to obtain electronic materials stored outside of the United States by service providers, the CLOUD Act reflects Congress's effort to modernize the law in light of current technological realities. While providing law enforcement the ability to compel a service provider under the SCA to produce electronic data stored outside the United States, the CLOUD Act also imposes some limitations, permitting service providers to challenge warrants or other legal process issued under the SCA in certain circumstances. For example, a service provider may seek to modify or quash a warrant or other legal process issued under the SCA on the basis of a conflict of law with a "qualifying foreign government," which is defined as a government with which the U.S. executive branch has entered into an executive agreement under the CLOUD Act. To successfully challenge such a warrant, a service provider must demonstrate that: (1) the customer or subscriber is not a "United States person," as defined, and does not reside in the United States; and (2) the required disclosure would create a material risk that the provider would violate the laws of the qualifying foreign government. While such a motion is pending, service providers must preserve, but are not obligated to produce, the information sought. A court may grant such a motion only if it finds that both of the above-referenced requirements are met and that, based on the totality of the circumstances, the "interests of justice" require that the warrant or legal process be modified or quashed. However, until such executive agreements have been executed with foreign governments and tested, it is uncertain whether this method for challenging the new SCA warrants will be a viable option for service providers.

In clarifying the ability of U.S. law enforcement to obtain electronic materials stored outside of the U.S. by service providers, the Clarifying Lawful Overseas Use of Data (CLOUD) Act reflects Congress's effort to modernize the law in light of current technological realities.

If the above circumstances do not exist, the CLOUD Act provides another potential mechanism, albeit ambiguous, for a service provider to challenge a data warrant. It states that U.S. law enforcement actions under Section 2703 of the SCA are to be evaluated by "the common law standards governing the availability or application of comity analysis." However, the judiciary and the CLOUD Act itself have not specifically defined what the comity analysis would entail, though the multi-factor balancing test established in *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for the S. Dist. of Iowa*, 482 U.S. 522 (1987), may be instructive here.

Conclusion

The *Microsoft* case brought attention to complex issues impacting collection of data from overseas, helping to spur Congress into action, resulting in the passage of the CLOUD Act. The act represents a significant change in the way in which the U.S. government can obtain information stored outside of the U.S. and the ability for service providers to object to such requests. It also provides much-needed clarity on the SCA's applicability in our current cloud-service provider era. That said, the CLOUD Act's ratification of the extraterritorial reach of the U.S. government in search warrants under the SCA may set the stage for future conflicts on the data privacy front, especially with EU countries and data subjects who may view the CLOUD Act as a governmental overreach that infringes on a fundamental right to privacy.