NICHOLS LIU

SERVING GOVERNMENT CONTRACTORS

CLIENT ALERT

Ominous CLOUD for Contractors Working Internationally

May 21, 2018

Can the government compel an email provider to produce emails stored overseas? The government believed that it could, under Section 2703 of the Stored Communications Act, 18 U.S.C. § 2701, *et seq*. (SCA or Section 2703). The Second Circuit disagreed in *United States v. Microsoft*, but before the Supreme Court could answer the question, Congress passed the CLOUD Act and rendered the case moot. That legislative amendment will be the *Microsoft* case's legacy: it is now clear that—absent countervailing comity concerns—the government can obtain emails and other data regardless of where they are stored physically.

This development is important for government contractors, especially for those which have offices or perform overseas, as it indisputably sweeps emails stored overseas into the ambit of the SCA.

The Stored Communications Act - Section 2703

The SCA authorizes the government to require providers of electronic communications, such as Microsoft, to disclose information to the government about wire or electronic communications, including emails. *See* 18 U.S.C. § 2703. Section 2703 provides three separate mechanisms for the government to acquire such information.

First, the government may issue an "administrative subpoena authorized by a Federal or State statute" or "a Federal or State grand jury or trial subpoena." *Id.* § 2703(b)(1)(B)(i). With a subpoena, the government may acquire basic subscriber information such as the subscriber's name and identifying information. *Id.* § 2703(c)(2). If the government provides prior notice to the subscriber, *id.* § 2703(b)(1)(B)—or complies with procedures that allow notice to be delayed by up to 90 days, *id.* § 2705(a)—it may also use a subpoena to obtain the contents of emails stored by an electronic communication service for more than 180 days. *Id.* § 2703(b)(1)(B)(i),

Second, the government may obtain a court order under Section 2703(b)(1)(B)(ii) for the same information obtainable by subpoena. Because the procedures for such an order must be sought under Section 2703(d), it is often called a "Section 2703(d) order." Under Section 2703(d), the government must "offer[] specific and articulable facts showing that there are reasonable grounds to believe that" the records sought are "relevant and material to an ongoing criminal investigation." *Id.* § 2703(d). The same notice requirement applies to email content. *Id.* § 2703(b)(1)(B). A Section 2703(d) order goes further than a subpoena, however, insofar as the government may also acquire "other information pertaining to a subscriber," beyond basic account information and the contents of emails. 18 U.S.C. § 2703(c)(1)(B).

Third, the government may obtain a "warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction" and thereby "require the disclosure" by a service provider of electronic communications and other records. *Id.* §§ 2703(a) (electronic communications in storage), 2703(b) (remote computing services), 2703(c)(1)(A) (subscriber information). Under a Section 2703 warrant, the government may demand any of the same records covered by a 2703(d) order—but without providing prior notice to a subscriber. *Id.* § 2703(b)(1)(A). In addition, unlike through subpoenas or Section 2703(d) orders, the government may obtain the contents of communications stored by an electronic communication service for fewer than 181 days. *Id.* § 2703(a). As with any warrant, the government must satisfy a neutral judicial officer that there is probable cause to believe that the records to be disclosed contain evidence of a crime, and the government must describe those records with particularity. *See* Fed. R. Crim. P. 41(d); U.S. Const. Amend. IV.

Background and Procedural History

When someone signs up for an MSN.com email account, she identifies which country she is from. Microsoft then migrates the account to a datacenter near the user's self-reported location, to reduce network latency. Microsoft keeps certain data sets in the United States—the user's address book; non-content email information; and the user's name and country—while other data sets are kept overseas. In the *Microsoft* case, the user reported Ireland as its location, and Microsoft migrated the email account to servers in Dublin.

On December 4, 2013, a federal magistrate judge in the Southern District of New York issued a Section 2703 warrant for the email account. Microsoft disclosed the account information that was stored in the United States but moved to quash the warrant as to all material stored abroad, arguing that it was an impermissible extraterritorial application of Section 2703. The motion was denied, and Microsoft was held in civil contempt. The magistrate concluded that Section 2703 does not "alter the basic principle"—which has "long been the law"—that "an entity lawfully

obligated to produce information" in its control "must do so regardless of the location of the information." 15 F. Supp. 3d 466, 472 (S.D.N.Y. 2014) (citing *Marc Rich & Co. v. United States*, 707 F.2d 663, 667 (2d Cir.), *cert. denied*, 463 U.S. 1215 (1983)). The district court affirmed the magistrate's ruling.

The Second Circuit reversed, concluding that enforcing the warrant as to information stored abroad would constitute an impermissible extraterritorial application of the statute. 829 F.3d 197, 222 (2d Cir. 2016). Reasoning that the primary goal of the SCA was the protection of privacy, *id*. at 217, and that any invasion of privacy through an SCA warrant would occur where the customer's protected content is stored, the Second Circuit concluded that the location of the *data*, not of the *customer*, governed the extraterritoriality analysis. *Id*. at 47a.

After the Second Circuit denied rehearing *en banc*, the government petitioned for writ of *certiorari*, which was granted. Oral arguments were heard on February 27, 2018. On March 23, 2018, Congress enacted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) as part of the Consolidated Appropriations Act, 2018, Pub. L. 115-141 (2018).

Arguments before the Supreme Court

All agreed that the SCA lacked the kind of clear statement that would overcome the default presumption against extraterritorial application of federal statutes. Thus, the critical question in *Microsoft* was whether compliance with the Section 2703 warrant was a domestic or an extraterritorial application of the SCA. Section 2703 was enacted against the backdrop of a historical, territorial limitation on search warrants. The Supreme Court has never upheld the use of a warrant to compel a recipient to produce an item under its control, but located overseas, when the recipient is merely a caretaker for another individual or entity and that individual, not the warrant's object, has a protectable privacy interest in the item.

The government argued that the focus of the statute is on "where the conduct occurred." Because the disclosure of records from Microsoft to the government would occur in the United States, the government argued that compliance with a Section 2703 warrant is a domestic, not an extraterritorial, act and that Microsoft can easily "collect" data stored abroad by inputting commands at its facility in the United States. As a policy matter, the government claimed that a contrary holding would invite even unsophisticated criminals to claim they were from another country to ensure that their data was stored overseas, thereby precluding government intrusion into their emails.

Microsoft argued that the focus of the SCA is on user privacy, and that it governs domestically *stored* communications, not domestically *disclosed* communications.

Vacating the Case

After Congress passed the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") on March 23, 2018 (less than a month after oral arguments were heard by the Supreme Court), the government moved to vacate the Second Circuit's decision in favor of Microsoft. The Cloud Act specifies that a service provider responding to a Section 2703 order must produce information within its "possession, custody, or control, regardless of whether such . . . information is located within or outside of the United States." *See* Clarifying Lawful Overseas Use of Data Act, H.R. 1625, Div. V, 115th Cong., 2d Sess. (2018). The government withdrew its previous warrant, rendering the case moot.

Microsoft agreed with the government that the CLOUD Act defines a new approach for balancing legitimate law-enforcement interests, individual privacy rights, and foreign sovereignty. Microsoft also agreed that there was no longer a live case or controversy between the parties.

The Court agreed and vacated the case by *per curiam* opinion on April 17, 2018.

Implications Going Forward

On March 30, 2018, the government served Microsoft with a new warrant, under the CLOUD Act, and Microsoft has indicated that it will "evaluate the new warrant as it evaluates all warrants that law-enforcement entities serve on it." In the meantime, the CLOUD Act has real implications for government contractors—especially in the international and foreign-development space. Whereas entities or individuals may have intentionally kept emails overseas, and thus arguably out of the government's reach, an email's physical location is no longer an automatic shield.

At the same time, the CLOUD Act is not a silver bullet for U.S. prosecutors. There is now a statutory comity analysis, under which a service provider subject to a Section 2703 subpoena or warrant may move to modify or quash it if the provider reasonably believes both that the customer whose data is requested is neither a U.S. person nor a U.S. resident and that "the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government." CLOUD ACT § 103(b), codified at 18 U.S.C. 2703(h)(2). Microsoft might avail itself of this section if compliance with the renewed warrant would create a material risk that Microsoft would violate the data protection laws of Ireland and the E.U. It is worth noting that the E.U. and its member countries generally have more protective privacy laws when

it comes to electronic communications, than does the United States. See, e.g., the EU's General Data Protection Regulation. Nevertheless, the scheme inherently depends on the *provider* raising arguments on the customer's behalf, which may offer little comfort to the average customer.

Contacts:

Andy Liu
202.846.9802
aliu@nicholsliu.com

Jason C. Lynch
202.846.9834
jlynch@nicholsliu.com

Rebekah Woods
202.846.9824
rwoods@nicholsliu.com