ALERT MEMORANDUM

CLOUD Act Establishes Framework To Access Overseas Stored Electronic Communications

April 4, 2018

The 2018 Consolidated Appropriations Act, which was signed by President Donald Trump on March 23, 2018, included a little-debated provision that revised portions of the 1986 Stored Communications Act ("SCA") to permit the government to access through the use of a warrant or subpoena stored communications held abroad by providers of electronic communications services that are subject to United States jurisdiction.

The Clarifying Lawful Overseas Use of Data Act – or "CLOUD Act" – establishes that the SCA's provisions concerning the production of electronic communications extend to those held abroad, establishes a framework for service providers to challenge an SCA warrant, directs courts to conduct a limited comity analysis to balance certain factors relevant to cross-border transfers of data, and introduces an incentive for foreign governments to enter into executive agreements with the United States governing cross-border data requests.

Prior to the enactment of the CLOUD Act, the Supreme Court was poised to rule in the case Microsoft Corporation v. United States of America, No. 17-2, on whether the SCA in its previous form permitted the use of a warrant to obtain electronic communications stored by a U.S. company on foreign servers. The relevance of that case, which was argued in February, is substantially undermined by this Congressional action.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or any of the partners and counsel listed under Litigation and Arbitration or White Collar Defense and Investigations in the "Our Practice" section of our website.

NEW YORK

Jonathan I. Blackman
+1 212 225 2490
JBlackman@cgsh.com

Jared Gerber
+1 212 225 2507
JGerber@cgsh.com

NEW YORK
One Liberty Plaza
New York, NY 10006-1470
T: +1 212 225 2000
F: +1 212 225 3999

WASHINGTON, D.C.

Nowell D. Bamberger
+1 202 974 1752
nbamberger@cgsh.com

WASHINGTON, D.C.
2000 Pennsylvania Ave. NW
Washington, D.C. 20006
T: +1 202 974 1500
F: +1 202 974 1999

The Stored Communications Act

Motivated by a concern that the increasing use of electronic communications placed electronic communications in the hands of third party service providers – and therefore arguably outside the scope of Fourth Amendment privacy considerations – in 1986 Congress adopted the SCA to impose statutory confidentiality obligations on providers of electronic communications services and prescribe the circumstances under which the government can compel production of remotely stored electronic communications.[1]

Prior to the enactment of the CLOUD Act, the SCA contained three principal substantive provisions:

- 18 U.S.C. § 2701, which creates a felony offense for intentionally accessing a facility through which an electronic communication service is provided;
- 18 U.S.C. § 2702, which prohibits providers of electronic communications services to the public from knowingly divulging the contents of electronic communications or other records, subject to a limited set of exceptions; and
- 18 U.S.C. § 2703, which prescribes detailed rules under which a government entity may require the disclosure by a provider of an electronic communications service of various information concerning electronic communications – including records concerning the sender or recipient of such communications, or the contents of such communications – and the mechanisms by which such communications can be accessed.

Section 2703, in turn, authorizes two separate means by which a government entity can request information from a provider of electronic communications. First, the government can obtain a warrant issued using the procedures described in the Federal Rules of Criminal Procedure, without notice to the subscriber or customer, to obtain the contents of such electronic communications. Second, with notice to the subscriber or customer, the government can obtain such records using an administrative or grand jury subpoena or a court order.[2] Other provisions govern the process applicable to requests for subscriber and record information other than the contents of electronic communications.

The SCA, before the Cloud Act, did not explicitly address whether and under what circumstances the government can require the production of electronic communications stored outside the United States.

Microsoft v. United States

In a much-watched case, the Supreme Court was poised to determine whether the government can use a warrant issued pursuant to Section 2703 of the SCA to access records held by a Microsoft affiliate in Dublin, Ireland. Central to Microsoft v. United States was whether a "warrant" issued pursuant to the SCA and directed to a U.S. company could lawfully compel a company to transfer into the United States communications that, although under its control, were outside the territorial jurisdiction of the United States. Microsoft argued that a "warrant" was, by definition, only enforceable within United States territory and that nothing in the SCA expressly spoke to any Congressional intent that the statute's disclosure mechanisms should apply extraterritorially.[3] The Government, in turn, argued that an SCA warrant is executed within the United States when it is served on a domestic company, and that upon such service, the SCA required respondents to obtain and produce

[1] S. REP. 99-541, 5, 1986 U.S.C.C.A.N. 3555, 3559 ("[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.").

[2] 18 U.S.C. § 2703(b)(1)(A–B).

[3] See Brief for Respondent at 11–14, United States v. Microsoft Corp., No. 17-2 (Jan. 11, 2018).

documents under its possession, custody or control, no matter where located.

The Microsoft litigation began in 2013 when the Government applied for a Section 2703 warrant under the SCA requiring Microsoft to disclose email communications for a particular user believed to be involved in illegal drug activity. Microsoft operates web-based email services that are free to the public. Data associated with these services (*i.e.*, email communications) are stored on servers at Microsoft datacenters around the world. In this case, the user's email content was stored on a server at a datacenter based exclusively in Dublin, Ireland. The Government served Microsoft at its corporate headquarters in Redmond, Washington, and in response Microsoft disclosed certain responsive account information that was stored in the United States. Microsoft, however, refused to turn over the user's email content stored in Dublin, and moved to quash the warrant, arguing that the SCA does not apply extraterritorially to data stored outside the United States.

In 2014, the U.S. District Court for the Southern District of New York declined to quash the government's warrant; the Second Circuit reversed in 2016,[4] a decision as to which the Government petitioned for a writ of certiorari, which was granted on October 16, 2017. The matter was argued on February 27, 2018, and more than twenty parties submitted briefing as amicus curiae.[5]

The CLOUD Act

The CLOUD Act was introduced on February 6, 2018, and until it was adopted had not received significant legislative attention. As of oral argument in the Microsoft case, the CLOUD Act had not received a committee hearing in either the House or Senate. It was therefore somewhat unexpected when the CLOUD Act was enacted as a provision of the must-pass 2018 omnibus appropriations bill.

In substance, the CLOUD Act introduces four principal changes to the SCA framework:

- Section 103 amends the SCA by adding a new section (Section 2713), which expressly states that the SCA applies extraterritorially. Section 2713 states that a service provider must comply with the requirements of the SCA to "preserve, backup, or disclose the contents of" electronic communications "regardless of whether such communication, record, or other information is located within or outside of the United States."[6]
- The same section also amends Section 2703 of the SCA to provide a mechanism for service providers to challenge or move to quash SCA warrants, a process that was previously lacking (traditionally, the only way to challenge a warrant without complying was to refuse compliance and litigate a contempt finding).[7]
- Newly-added Section 2703(h) requires a court confronted with a request for communications located abroad to conduct a limited comity analysis considering any potential penalties arising by virtue of inconsistent legal obligations, and the interests of certain foreign governments.
- Section 105 introduces a new statutory provision – Section 2523 – that defines criteria for executive agreements between the United States and other governments governing cross-border requests for information, and authorizing providers of electronic

---

4 See Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016).

5 This includes Brief for Amicus Curiae European Company Lawyers Association in Support of Respondent, United States v. Microsoft Corp., No. 17-2 (Jan. 18, 2018); Brief of the Council of Bars and Law Societies of Europe as Amicus Curiae in Support of Respondent, United States v. Microsoft Corp., 17-2 (Jan. 18, 2018).

6 CLOUD Act § 103(a)(1); to be codified at 18 U.S.C. § 2713.

7 See CLOUD Act § 103(b); to be codified at 18 U.S.C. § 2703(h)(2).

communications service to respond to requests by foreign governments pursuant to such agreements without violating the SCA.

Express Extraterritoriality

Mirroring many of the arguments advanced by the Government in the Microsoft litigation, Section 102 demonstrates that one purpose of the CLOUD Act's extraterritoriality provision is to reduce barriers to law enforcement investigations. In its preamble, Section 102 of the CLOUD Act states that timely access to electronic data held by service providers is "essential" to law enforcement, but that the U.S. government's efforts are "being impeded by the inability to access data stored outside the United States."[8] Section 102 further acknowledges that service providers may face conflicting laws when they are asked to disclose communications that are stored abroad. Following that rationale, the CLOUD Act adds Section 2713 to the SCA, which requires that service providers comply with the SCA's obligations to disclose a customer's communications even if those communications are "located . . . outside of the United States."[9]

However, Section 2713's extraterritoriality does not extend to Section 2702 of the SCA, which prohibits a service provider from disclosing a customer's communications unless authorized by an exception.[10] The CLOUD Act therefore appears to create an asymmetry in how service providers subject to U.S. jurisdiction must treat data stored abroad: such data *is* subject to the disclosure requirements of the SCA, but not to the provisions that protect customers against the disclosure of their information. As a result, the CLOUD Act does not appear to preclude service providers that hold U.S. subscriber communications abroad from voluntarily disclosing such information.

Mechanism For Quashing A Warrant

Prior to the CLOUD Act, the SCA created differential treatment of service providers depending on whether the government requested a warrant or a subpoena. Crucially, while there is a well-established process for challenging a subpoena prior to enforcement, there is no pre-enforcement mechanism for challenging a warrant. In the non-SCA context, that it unsurprising – subjects of warrants rarely know that a warrant is being sought, and warrants are typically executed by law enforcement seizing the items enumerated in the warrant (as opposed to requesting that the subject collect and produce such records).

The CLOUD Act remedies the lack of a pre-enforcement mechanism for challenging enforcement of SCA warrants by creating a procedure by which service providers may petition a federal district court to quash SCA warrants where it believes:

> (1) "the customer . . . is not a United States person and does not reside in the United States; and"
>
> (2) "that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government."[11]

The Act provides, moreover, that the court may *only* quash a warrant if it finds that:

> (1) the disclosure would cause the provider to violate a foreign government's laws;
>
> (2) "based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and"
>
> (3) "the customer . . . is not a United States person and does not reside in the United States."[12]

---

8 CLOUD Act § 102(1–4).

9 CLOUD Act § 103(a)(1); to be codified at 18 U.S.C. § 2713.

10 See 18 U.S.C. § 2702(a–b).

11 See CLOUD Act § 103(b); to be codified at 18 U.S.C. § 2703(h)(2)(A–B).

12 Id.

Notably, the SCA as amended by the CLOUD Act continues to lack a mechanism for subscribers or customers to challenge SCA warrants pre-enforcement.

Required Comity Analysis

Under the CLOUD Act, the second factor of the court's analysis about whether to quash a warrant requires that the court undertake a comity analysis. The CLOUD Act amends Section 2703 of the SCA to require a comity analysis under the "totality of the circumstances."[13] These factors include:

> (1) "the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;"
>
> (2) "the interests of the qualifying foreign government in preventing any prohibited disclosure;"
>
> (3) "the likelihood, extent, and nature of penalties to the provider or any employees . . . as a result of inconsistent legal requirements . . .;"
>
> (4) "the location and nationality of the . . . customer whose communications are being sought . . . and the nature and extent of the . . . customer's connection to the United States . . . ;"
>
> (5) "the nature and extent of the provider's ties to and presence in the United States;"
>
> (6) "the importance to the investigation of the information required to be disclosed;"
>
> (7) "the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and"
>
> (8) "if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority . . . ."[14]

Most significantly, the CLOUD Act will now require courts to take into account both the interests of the United States and of foreign governments in determining whether to block a warrant, while also considering other factors, such as the effect of conflicting laws.

Executive Agreements Governing Cross-Border Requests

Section 105 of the CLOUD Act amends Title 18 of the U.S. Code by adding Section 2523, which grants the Attorney General the power to enter into executive agreements with foreign governments, provided that those foreign governments meet certain privacy and human rights requirements.[15] These requirements include that the foreign government must "afford[] robust substantive and procedural protections for privacy and civil liberties in light of the data collection" and must "adhere[] to applicable international human rights obligations."[16] If the foreign government meets these requirements, then the executive agreement reached between the United States and the foreign country allows for reciprocal data sharing, permitting both the United States and other foreign countries to access and share data stored abroad.

However, Section 2523 does place some restrictions on what foreign governments can ultimately access. For example, Section 2523 prohibits the foreign government from "intentionally target[ing] a United

---

13 CLOUD Act § 103(b); to be codified at 18 U.S.C. § 2703(h)(2–3).

14 CLOUD Act § 103(b); to be codified at 18 U.S.C. § 2703(h)(3).

15 See CLOUD Act § 105(a); to be codified at 18 U.S.C. § 2523.

16 CLOUD Act § 105(a); to be codified at 18 U.S.C. § 2523(b)(1), (b)(1)(B)(iii).

States person or a person located in the United States."[17]

Implications of the CLOUD Act

While it remains to be seen the extent to which the SCA, as amended by the CLOUD Act, will continue to produce the types of legal conflicts which were the basis of the Microsoft litigation, the statute now supplies a new procedure for challenging a warrant under the SCA, significantly expands the scope of the SCA's data access provision, and recognizes the importance of respecting foreign sovereignty in executing data requests pursuant to the SCA.

We expect a number of implications to follow:

First, on March 30, the Government filed a motion requesting that the Supreme Court vacate the judgment in the Microsoft case and remand the case for dismissal by the lower courts in light of an intervening change in law. On April 3, 2018, Microsoft filed a response stating that it will not oppose the motion, noting that the Government has since withdrawn the original warrant that was the basis of the litigation and obtained a new warrant issued pursuant to the CLOUD Act.

Second, by introducing a procedure for pre-enforcement challenges to SCA warrants and requiring a comity analysis, the CLOUD Act effectively aligns the SCA warrant procedure with well-established procedures for enforcing subpoenas and civil discovery requests with respect to information held abroad by entities otherwise subject to U.S. jurisdiction. That approach, which follows the Supreme Court's decision in Société Nationale Industrielle Aérospatiale v. United States District Court, 482 U.S. 522 (1987), is a familiar balancing analysis under which courts more often than not compel production of information held abroad in the absence of clear evidence of imminent penalties arising from such disclosure. Indeed, insofar as the subpoena procedure under the SCA already permitted the government to request communications held abroad by companies subject to U.S. jurisdiction, we do not expect the CLOUD Act will significantly alter the landscape of cross-border enforcement.

Third, the SCA amendments may encourage some foreign firms to avoid storing their information with U.S.-based service providers or service providers that operate in the United States, on the grounds that doing so exposes such communications to compulsory U.S. legal process even if the relevant records are held exclusively outside the United States.

Fourth, while the CLOUD Act does appear to incentivize agreements between countries to share data by permitting consideration of foreign interests as part of a comity analysis only to the extent the foreign government has entered into such an agreement, it is also the case that some countries maybe be unable to enter into such agreements with the United States due to restrictions under their domestic law. For example, under China's recently-enacted cybersecurity legislation, China's critical network infrastructure firms are *prohibited* from transferring data to authorities abroad; that restriction would seem to preclude China from entering into an agreement with the United States that would satisfy the provisions of the CLOUD Act. The situation in the European Union is not substantially different, insofar as the incoming General Data Protection Regulation ("GDPR") will preclude reliance on a foreign legal request to transfer personal information abroad in a manner otherwise inconsistent with the GDPR.[18] It therefore remains to be seen how effective Section 105 of the CLOUD Act will be in encouraging foreign governments to enter into executive agreements governing cross-border data transfers.

…

CLEARY GOTTLIEB

[17] CLOUD Act § 105(a); to be codified at 18 U.S.C. § 2523(b)(4)(A).

[18] Article 48 of the GDPR.