Storm Clouds or Silver Linings?

The Impact of the U.S. CLOUD Act

FREDERICK T. DAVIS AND ANNA R. GRESSEL

The authors are with Debevoise & Plimpton LLP in Paris and New York City, respectively.

In March 2018, President Trump signed a $1.3 trillion annual appropriations bill. Wedged into its 2,232 pages, and unseen by nearly everyone, was the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act), which sets far-reaching new rules for international cooperation by criminal investigators seeking emails and data from foreign countries.

The act fills gaps highlighted during the recent Supreme Court oral argument in *United States v. Microsoft*. That case pressed the justices to interpret the 1986 Stored Communications Act (SCA) in light of new and rapidly evolving technology. The Supreme Court never decided the *Microsoft* case. Instead, the Court dismissed it as moot after the CLOUD Act was enacted.

While the CLOUD Act provides innovative new approaches to some of the criminal investigation challenges posed by technology, it naturally also raises new questions and concerns. The fact that most information is digitized (that is, recorded as bytes), the ubiquity of the Internet, and fast-paced globalization complicate traditional approaches to obtaining information in criminal investigations because data may be stored in a different country than the person or entity seeking it.

In the course of a criminal or regulatory investigation, police, prosecutors, and others routinely need access to private information held by a person being investigated or by a third party. The procedures for them to do this are well known: Investigators can obtain a subpoena, warrant, or other order from a local authority; effect service subject to the jurisdiction of that authority; and either compel the recipient to turn over the information or authorize a local official to seize it.

The fact that personal information such as emails and financial data such as bank accounts are digitized does not by itself interfere with traditional procedures for obtaining information. A bank or a communications company can be served with an order directing production of relevant information it stores as data. Conceptually, the process is not much different from procedures to obtain paper or other physical evidence. And the practices established by the relevant legal authorities provide procedural regularity, privacy protection, and appropriate transparency.

Entirely new problems arise, however, when the data in question are physically stored in a location subject to the laws of a different country. Now the issue is not just privacy—and how to balance the legitimate needs of the state and the protectable interests of the individuals—but also sovereignty. What country's laws and procedures should govern? This phenomenon is broadly known as the "deterritorialization of data," and in the view of some, it is a fundamental threat to sovereignty itself.

The express goal of the CLOUD Act is to take the lead in establishing a new international regime for cross-border data requests by law enforcement agencies by addressing gaps in the SCA that

Published in *Litigation*, Volume 45, Number 1, Fall 2018.

were exposed in the *Microsoft* litigation. While the CLOUD Act modernizes certain procedures and standards, questions remain about its scope, how it will be implemented domestically, and its impact on the existing mutual legal assistance treaties (MLATs) and letters rogatory that have been the traditional means of cross-border law enforcement cooperation.

The European Union (EU) has its own competing draft legislation addressing cross-border investigations. Given that, and in light of the restrictions on data transfers established in the new EU General Data Protection Regulation (GDPR), will the CLOUD Act be effective in setting an international standard for cross-border law enforcement investigations?

United States v. Microsoft

United States v. Microsoft called into question the SCA's extraterritorial reach. The *Microsoft* case arose from a typical drug-trafficking investigation of "John Doe." In 2013, after investigators established probable cause that Doe had used a Hotmail account in furtherance of a drug-trafficking offense, U.S. prosecutors served Microsoft with a warrant issued under specific SCA procedures governing access to stored data. The warrant directed Microsoft to turn over Doe's emails.

Microsoft promptly turned over Doe's subscriber information but refused to produce the content of Doe's emails. Because Doe had identified himself as a citizen of Ireland when he created his Hotmail account, Microsoft stored the contents of his emails on its server in Dublin, under its standard policy to store data close to the user to minimize delay (or what's known as "latency") in the time required to store or retrieve the data.

As to those emails, Microsoft moved to quash the SCA warrant. Microsoft argued that the SCA did not have extraterritorial effect and could not compel a U.S. service provider to turn over data stored in a foreign country. Microsoft contended that the prosecutor needed instead to pursue an MLAT or other means of obtaining cooperation from authorities in Ireland.

The District Court for the Southern District of New York ordered Microsoft to comply, finding that disclosure to the Department of Justice (DOJ) by a U.S. company of data under its custody and control did not require extraterritorial application of the SCA regardless of where the data were stored. The court focused on the uncontested fact that Microsoft "controlled" the Irish-located data, in the sense that at all times Microsoft had ready access to it from the United States. From this, the district court reasoned that there was no real issue about the "extraterritorial" effect of a U.S. warrant because the warrant would be executed *inside* the United States and no steps necessary for its execution would take place abroad.

The Second Circuit reversed, holding that an SCA warrant could not compel disclosure of emails stored in Ireland. The court found that the presumption against exterritorial application emphasized by the Supreme Court in *Morrison v. National Australia Bank*, 561 U.S. 247 (2010), applied to the SCA, as there was no indication of extraterritorial intent in the SCA's text or legislative history. In so ruling, the Second Circuit reasoned that the key issue is not where the data are accessed or disclosed, but rather where the data are stored.

In October 2017, the Supreme Court granted certiorari, in what became a much-discussed case with high stakes for both the law enforcement and technology sectors, in addition to its implications for individual privacy. The appeals caused an unusual number of briefs to be filed by *amici curiae*. They generally fell into four groups:

- prosecuting offices, which supported the DOJ's insistence that the SCA must be interpreted to give access to data stored abroad if accessible from the United States;
- the Republic of Ireland and representatives of the European Union, which expressed concern over infringement of their sovereignty, often noting that privacy is protected differently and generally more zealously in Europe than in the United States;
- technology and communications companies, which backed Microsoft's insistence that data stored abroad should not be subject to U.S. procedures; and

Illustration by Sawsan Chalabi

- privacy-oriented nongovernmental organizations, which viewed the limitation on the SCA warrants as necessary to protect against cross-border invasions of privacy.

During the appeals, an interesting new element complicated everything. In an unrelated but similar case, a prosecutor in Philadelphia sought emails of a Google customer. *See In re Search Warrant No. 16-960-M-01 to Google*. When served with an SCA warrant, Google raised Microsoft's arguments that it should not have to comply, arguing that the email data were not stored in the United States.

Unlike in the *Microsoft* case, in which the data had a definite location on servers in Ireland, the Google email data were broken into "shards," which were stored on different servers in different locations on a frequently changing basis as managed by an algorithm designed to improve efficiency. This was a new step on the road to "deterritorialized data" because they had no identifiable "location" at all and no single national regime such as Ireland could assert a sovereign interest in the data based on their location.

With unusual speed and no debate, and before the Supreme Court could issue its ruling in *United States v. Microsoft*, Congress passed the CLOUD Act as part of an omnibus spending bill, which was then signed into law by the president. The act had the apparent support of both the DOJ and Microsoft, among other service providers.

On the issue squarely raised in the *Microsoft* appeal, the act provides a clear answer, though it raises new questions as well. Specifically, if a service provider located in the United States receives an SCA warrant, the service provider no longer can argue that the data, while accessible from the United States, cannot be reached under the SCA because they are stored abroad. The CLOUD Act expressly provides that the service provider must "preserve, backup, or disclose" data responsive to an SCA warrant or subpoena that is in the "provider's possession, custody, or control," regardless of whether the data are located domestically or outside the United States.

That legislative language provided the clear congressional intent for extraterritorial application of the SCA that the Second Circuit had found lacking. Thus, for Microsoft and any other U.S. service providers, the legal terrain is now clear—they must disclose any data within their possession, custody, or control, irrespective of where those data are stored. Once the DOJ issued a new warrant for the John Doe material stored in Ireland and Microsoft recognized its validity, the Supreme Court dismissed the case as moot.

In the vast majority of cases, a U.S. service provider receiving an order to produce data will simply do so because there will be no legal basis not to. In the narrow range of cases that involve identifiable foreign interests, the act specifies that a U.S. provider may challenge an SCA order by moving to quash it if the request implicates the interests of a friendly foreign government.

Specifically, the act allows a provider to demonstrate that it "reasonably believes" that the customer or subscriber is not a U.S. person and does not reside in the United States, and that the disclosure would cause a "material risk" that the provider would violate the laws of what's defined as a "qualifying foreign government" (or QFG), which we discuss shortly.

The act then introduces a new and innovative standard for review, providing that if the foreign citizenship of the data owner and a "material risk" of foreign prosecution are present, the court may find that "interests of justice" dictate that the order should be modified or quashed. The act establishes a seven-factor "comity analysis," to be used in determining what "interests of justice" to consider, and the analysis includes evaluating the nature and extent of the subscriber's contacts with the United States and the QFG and the importance of the information to the investigation, among other factors. By introducing such a comity analysis, the act offers limited but express recognition that other countries may have a legitimate interest in whether data owned by their citizens can be seized by U.S. authorities.

Addressing one question, the act leaves open another: While all U.S.-based service providers must comply with the CLOUD Act, does it also apply to non-U.S. service providers? The act does not say. Application may depend on an analysis of whether the service provider is "subject to the jurisdiction" of the United States by doing business here.

What will happen, for example, if a non-U.S. service provider stores its data outside the United States and neither maintains an office here nor regularly markets its services here? Because the Internet is ubiquitous, a non-U.S. customer of such a provider could nevertheless access and use his emails while physically located in the United States, committing a crime or participating in criminal activity having effects here that might subject him to criminal prosecution.

If a U.S. prosecutor then investigated that crime and sought the incriminating emails, the prosecutor might face difficulties in arguing that the SCA (even as amended by the CLOUD Act) requires that service provider to turn over its data if the provider, in turn, argues that it is not subject to U.S. jurisdiction.

This is not merely an academic issue. Given that prospective lawbreakers often can *choose* where their data are stored, they may have an incentive to select non-U.S.-based service providers with no presence in the United States in the hope that U.S. authorities will be unable to bring the new pressure available under the CLOUD Act to bear on them to produce evidence. In fact, it is likely that the perceived competitive disadvantages of an adverse ruling in the *Microsoft* case triggered the technology industry's massive support of Microsoft's position through the filing of amicus briefs.

The act also does not address what happens if a U.S. service provider seeks to quash a warrant or subpoena when it is at risk of foreign prosecution by a government that has *not* qualified as a QFG. In that circumstance, the service provider might argue that a common-law comity analysis should fill this gap, but a court might reason that Congress's silence intended to limit such comity deference to only QFGs.

Foreign Governments and U.S. Entities

While the *Microsoft* case involved data sought by U.S. law enforcement authorities, a separate but now linked issue is if (and how) *non*-U.S. authorities can get access to data that are stored in the United States or are under the control of U.S. entities.

Before the CLOUD Act, the SCA categorically prohibited U.S. companies from disclosing content such as emails directly to foreign governments, thus requiring such governments to use MLATs or other procedures. If a foreign power issued a court order directing Microsoft to disclose email content of a U.S. person, Microsoft might have faced the unenviable choice of violating U.S. law or violating foreign law. In practice, that meant that foreign governments generally transmitted data requests to the U.S. government under an MLAT or a letter rogatory so that the U.S. government could seek the data from the U.S. provider on the foreign government's behalf.

The EU is currently considering legislation that would operate similarly to the CLOUD Act.

While the MLAT and letter rogatory processes are generally effective, reaction times can be slow even for critical and time-sensitive requests. To encourage international cooperation and to counterbalance its extension of U.S. authority, the CLOUD Act introduces an alternative system for foreign law enforcement data requests.

The CLOUD Act allows certain foreign governments to enter into executive agreements with the U.S., thereby becoming "qualifying foreign governments." QFGs effectively prequalify to serve foreign law-enforcement requests *directly* on U.S. service providers, rather than via the U.S. government as an intermediary.

The CLOUD Act expressly lifts the SCA's prohibitions on disclosure directly to QFGs, which allows—but does not by itself compel—a U.S. provider served with such a foreign order to turn over data to the QFG without fear of penalty.

To qualify as a QFG, a foreign government must enter into an executive agreement under the CLOUD Act, pursuant to which the attorney general, with the concurrence of the secretary of state, must certify to Congress that the potential signatory government satisfies certain requirements, such as that it "affords robust substantive and procedural protections for privacy and civil liberties" and has "appropriate" data protection procedures regarding retention, acquisition, and dissemination of data regarding U.S. persons.

The CLOUD Act provides for a 180-day expedited review process during which Congress has the power to prevent a proposed executive agreement from coming into effect. The certifications are to be renewed every five years, at which time Congress again has the power to prevent renewal through a joint resolution disapproving the proposed executive agreement.

The QFG carve-out permitting foreign governments to serve their orders directly on U.S. service providers is limited to situations in which the orders relate to a serious crime, including but not limited to terrorism; identify a specific person, account, or other entity that is the object of the order; are justified by "articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation"; and, in the case of interception of wire or electronic communications, are of a fixed and limited duration, last only as long as reasonably necessary, and are to be issued only if information could not be obtained by a less intrusive method.

In addition, a QFG order must comply with the domestic law of the issuing country, may not be used to infringe on freedom of speech, and may not target a U.S. person.

Unsurprisingly, given the speed of its drafting process, the CLOUD Act does not fully address how these executive agreements will work in practice. For example, the act provides no procedure for a recipient of an order from a QFG to contest that order in a U.S. court. That seems odd. As the act specifically limits the circumstances under which a QFG can directly serve an order on a U.S. service provider, a domestic mechanism should exist to test whether those conditions have been met.

Moreover, the act provides that "the United States Government shall reserve the right to render [an executive agreement] inapplicable as to any order for which the United States Government concludes the agreement may not properly be invoked." While that clearly empowers the executive branch to intervene in cases when a QFG request is deemed inappropriate, the act does not specify what effect such an intervention will have.

Responses to the CLOUD Act

Responses to the CLOUD Act have ranged from enthusiastic support to ambivalence to harsh critique. Law enforcement officials argue that the act has solved the policy issues raised by the Second Circuit decision in *Microsoft*. Service providers hope that CLOUD Act executive agreements will limit the circumstances under which they are forced to choose between violating U.S. law and violating foreign law. And both groups believe that the data-sharing process under the CLOUD Act is more streamlined than the prior MLAT system, and that the act's procedures allowing QFGs to obtain data directly from private companies will fend off burdensome and privacy-threatening data-localization laws.

On the other hand, privacy advocates such as the American Civil Liberties Union and the Electronic Frontier Foundation express concern that the act does not adequately protect individuals' privacy interests. Notably, the CLOUD Act allows for QFGs to issue data using a standard that appears to be lower and broader than "probable cause," although some commentators suggest that the new standard is meant to encompass potentially varied foreign articulations, while the certification process ensures that those standards are adequate.

Meanwhile, organizations like Human Rights Watch have expressed concern that countries with relatively poor human rights credentials could be nonetheless certified as QFGs and thus granted broad access to individuals' data.

More broadly, the CLOUD Act represents a first step in what may be a paradigm shift in how access to digitized data is regulated. The *Microsoft* decisions were inherently premised on the presumption that data have specific locations and that these locations are relevant to determining whether a government has the power to compel their disclosure. Microsoft and Ireland asserted that Ireland had an interest in protecting the privacy of Irish citizens because the data were physically present there, likening the compelled production of Irish data stored on Irish servers to an invasion of their territory.

The DOJ's argument was similarly location-centric, although it argued that the location of the *disclosure* within the United States, not the storage of the data in Ireland, determined whether Microsoft could be compelled to produce the data, absent extraterritorial application of the SCA.

By expressly making the SCA extraterritorial, the CLOUD Act has reduced the relevance of data *location* and instead emphasizes *access*. If a service provider is subject to the jurisdiction of the United States, it now can be compelled to disclose data within its "possession, custody or control," regardless of the location of those data.

The CLOUD Act did not, however, fully account for the evolving nature of data storage and protection. So open questions remain as to its practical application.

The new act appears to address the issue of dynamically stored data—that is, data that are in near-constant motion from server to server, ike in the Google email case. Because such dynamically stored data have no fixed location, the applicability of SCA procedures to them was unclear. Now such data are responsive to U.S. warrants and subpoenas as long as they can be accessed from the United States.

Dynamically located data nonetheless may pose problems for the enhanced comity analysis afforded to QFGs that have entered into CLOUD Act agreements. As noted, a service provider receiving a domestic order may move to modify or quash it if, among other factors, the request would implicate the laws of a QFG. But that raises the issue of whether "the laws of a QFG" in fact apply to the data at all, which might not be the case if only a "shard" of a communication ever was stored in the foreign country, or if data were stored there only briefly and in transit.

To resolve that question, a court would need to apply the law of the QFG, which may or may not clearly resolve the issue. EU law, for example, is relatively clear. Under the GDPR, data collected in the European Union are considered EU data regardless of where they are stored. That makes the data storage location irrelevant. It remains to be seen, however, whether the laws of all nations that enter into CLOUD Act agreements will prove similarly sufficient to resolve this issue.

In addition, some companies may seek a competitive advantage by appealing to privacy-minded consumers by placing themselves outside the SCA's reach by avoiding any U.S. presence or by using technological measures to keep the U.S. government from being able to read their clients' data.

Some companies offer end-to-end encryption such that no one—not even the service provider—can open it without the key maintained by the client. The compatibility of such encryption and the fear of law enforcement agencies "going dark" because of easy availability of that technology are other issues now under scrutiny. In a recent non-SCA case, the Federal Bureau of Investigation (FBI) ordered Apple to decrypt the iPhone of a terrorism suspect. Apple resisted, arguing that it did not have the key to the phone locking mechanism. The FBI ordered Apple to develop a program that would break through that technological barrier. Ultimately, the issue was mooted when the FBI gained access to the phone through other means.

Outside the United States, countries may also take steps to protect data collected in their territory or deemed of interest to their citizens. Some countries are considering "localization" requirements that any data relating to a service offered in the country must be stored in that country.

Another option is the mandatory use of so-called "data trusts," under which local law would provide that data relating to communication services offered to citizens of a country would not be stored by the service provider at all, but would be automatically

transferred to a "trustee," accountable to that government, who would store the data on independent servers.

Under such data trusts, if the service provider were served with process under the SCA to disclose such data, it presumably would argue that it does not have possession, custody, or control of the data, but rather the trust does, and by local law the trustee may refuse any access that does not comply with local laws and procedures.

Internationally, responses to the CLOUD Act have been mixed. The United Kingdom has expressed support. Given that 90 percent of its suspects use U.S. communications services, the CLOUD Act could significantly streamline its own law enforcement investigations.

In contrast, during the *Microsoft* litigation, EU representatives submitted an amicus brief claiming that extraterritorial effect of the SCA by U.S. law enforcement without consideration of foreign laws would be a violation of sovereignty. The EU representatives also argued that the mandatory disclosure provisions of the SCA would potentially violate Article 48 of the EU's GDPR. The GDPR contains a blanket prohibition against transferring EU data outside the EU unless that transfer is authorized by an exception (or "derogation"). Those provisions in the GDPR maximize the protections granted to the customer and may make it difficult for EU member states to enter into CLOUD Act executive agreements with the U.S.

While certain derogations to Article 48 might allow a service provider to comply with U.S. data orders without violating the GDPR, the applicability of those derogations to requests under the CLOUD Act is uncertain. Notably, a QFG that enters into a CLOUD Act executive agreement must provide the U.S. with "reciprocal rights of data access." That presumably means that the U.S. would have the right to issue data orders directly to companies in the QFG, just as the QFG is permitted to do with regard to U.S. companies under the CLOUD Act.

While ultimately the scope of those reciprocal rights will be determined by each executive agreement, it may be difficult for any individual EU member state to grant such rights to the United States in light of the GDPR. EU member states are not permitted to offer less protection than what is mandated under the GDPR, making it complicated for a member state to unilaterally guarantee that data transfers under a CLOUD Act executive agreement would be permitted under a derogation to the GDPR.

Crucially, such extensive access to EU data by U.S. law enforcement may simply not be palatable, given the European focus on individual privacy rights.

It therefore remains to be seen whether the CLOUD Act signifies a new international model for cross-border law enforcement requests or whether it will simply be a Band-Aid fix for the specific issues presented in *United States v. Microsoft*.

All signs point to the United Kingdom entering into a CLOUD Act agreement with the United States shortly after it separates from the European Union. The impact of the CLOUD Act in continental Europe is more complicated; while the United States is now the first mover in this space, the U.S. perspective on data privacy differs dramatically from the European point of view, and it is not a given that the EU will accept the CLOUD Act as the basis for a new international law enforcement regime.

Indeed, the EU is currently considering legislation, called the e-Evidence Directive, that would operate similarly to the CLOUD Act. That draft legislation would require overseas companies to appoint a legal representative in the EU who could provide access to data stored outside the EU within 10 days of a request, or within six hours in the case of an emergency. The directive would apply to companies like Facebook and Google that offer services in the EU and have a "substantial connection" to the EU, meaning that the company either has an establishment in an EU country or provides services to a large number of users in an EU country.

Effectively, that would expand the EU's capacity to compel the disclosure of data held outside the EU, similar to the extraterritorial impact of the CLOUD Act.

It also remains to be seen how the CLOUD Act and the GDPR will evolve and interact. The European Union has the power to negotiate on behalf of all of its member states, granting it leverage of its own. At this nascent stage, it is far from clear which—if either—regime ultimately will provide the predominant model.

One thing is certain: The situation is fluid and will continue to evolve. Much of business, financial, and personal life now resides in data, and data no longer have a comfortable or intuitive connection to an identifiable "place" whose laws can be expected to regulate access to the data while also protecting the personal and business interests inherent in them.

Domestically, one can expect that constitutional protections of privacy will to some degree evolve with technology. In June 2018, the Supreme Court in *Carpenter v. United States* held for the first time that ad hoc government access under the SCA to cell phone "metadata"—which do not reveal the content of communications, but which do reveal objective facts such as location or identity—may be governed by the Fourth Amendment, despite the fact that the data are held by a third party.

Internationally, however, the problem remains complex. As data become simultaneously globalized and "deterritorialized," each country's judgment about how to balance investigative needs against privacy rights must increasingly take account of the rights and interests of other countries.

As the CLOUD Act shows, international cooperation on regulating data access is key. ■