Cyberspace LAWYER

April 2018 ▪ Volume 23 ▪ Issue 3

OVERSEAS DATA SEIZURES—U.S. SUPREME COURT HEARS ORAL ARGUMENT, BUT CONGRESS MIGHT GET TO THE ISSUE FIRST

by Steve Nickelsburg, Joshua Berman, Megan Gordon, Daniel Silver, Glen Donath & Adam Goldstein

Steve Nickelsburg (steve.nickelsburg@cliffordchance.com), Joshua Berman (joshua.berman@cliffordchance.com), Megan Gordon (megan.gordon@cliffordchance.com) and Glen Donath (glen.donath@cliffordchance.com) are Partners and Adam Goldstein (adam.goldstein @cliffordchance.com) is an Associate in the Washington, D.C. office of Clifford Chance. Daniel Silver (daniel.silver@cliffordchance.com) is a Partner in the firm's New York City office.

Introduction

When and how can the long arm of the U.S. government access customer data sitting outside of the United States? And what does this mean for the numerous global companies that store consumer data, and for the data of billions of customers around the world? This week, the U.S. Supreme Court heard arguments on these very questions in *United States v. Microsoft*.

Microsoft challenged a warrant from U.S. criminal authorities requiring the tech company to produce customer data stored on servers outside of the United States. Microsoft pits arguments for data privacy against those for investigative practicality and raises questions about how to control data across international borders. Although the Justices expressed varying policy concerns, the dispute focuses on interpretation of a 1986 statute in the current digital age—and could be resolved if Congress were to pass the Clarifying Lawful Overseas Use of Data ("CLOUD") Act before the Court issues its opinion by late June.

Background

The *Microsoft* case began in 2013 when the U.S. Department of Justice ("DOJ") served a warrant ordering Microsoft to produce a customer's "MSN.com" e-mails in relation to a drug prosecution. The U.S. government sought the warrant under the Stored Communications Act ("SCA"), enacted in 1986 to protect electronic data from unauthorized access, while allowing the government to require disclosure of such information pursuant to a warrant or court order.

Microsoft provided the DOJ with data stored on servers located in the United States. However, the company refused to provide data hosted on a server in Ireland, and moved to quash the warrant on the ground that the SCA does not apply to data stored outside the United States since

the statute does not explicitly provide for its extraterritorial reach. The District Court denied the motion to quash, and ordered Microsoft to produce the data stored in Ireland. The U.S. Court of Appeals for the Second Circuit reversed, ruling that "the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States."

Last October, the Supreme Court agreed to resolve this issue. In a relatively

unusual step—further highlighting the importance and broad applicability of the issues at stake—the Supreme Court agreed to hear this case even though there was not a split of opinions among the circuit courts.

The case has attracted significant international attention, with numerous foreign governments filing amicus curiae briefs offering various perspectives on the handling of data across borders. Technology and privacy organizations also filed amicus curiae briefs, illustrating the importance of the issue in light of the technology sector's increasing use of cloud storage across territorial boundaries.

Dueling Positions

In briefing and at oral argument, following a line of precedent regarding the extraterritorial application of U.S. law, the United States and Microsoft agreed that the SCA cannot apply extraterritorially because Congress did not explicitly state an intention for a statute to apply outside the United States. The parties disagreed, however, on whether the case actually involves the extraterritorial application of law.

The United States argued that Microsoft's disclosure would involve primarily domestic conduct—the production of evidence within the United States by an entity located in the United States in connection with a U.S. criminal investigation. Urging the Court to compel disclosure of data within the party's control—irrespective of the data's physical location—the United States explained thatMicrosoft could obtain and produce the data from a location in the United States, rendering the application of the law domestic. According to the government, any other interpretation would severely limit important tools for law enforcement.

Microsoft stressed that the purpose of the SCA was to protect stored data, not to encourage disclosure. According to Microsoft, because the data requested is stored abroad, the company would have to search through servers located overseas to locate and retrieve the data, making any required disclosure tantamount to an improper extraterritorial seizure.

Supreme Court Argument

While the Justices' questions at oral argument are not a guarantee of their ultimate positions or the outcome of the matter, they often shed some light on their thinking on the issues presented.

At the argument's outset, Justice Sotomayor jumped in to challenge the government's position that the issue centered on disclosure, voicing the view that the warrant is "really a search"—it allows the government, should it choose, to "go in, sit down at Microsoft's facilities, put hands on keyboards." Justice Gorsuch expressed similar doubts that disclosure is independent from collection, highlighting the "chain of activity," through which materials would "be collected

abroad and transmitted . . . to the United States." Justice Gorsuch pointed out that, before a party can "disclose, [the statute] anticipates necessarily certain antecedent conduct"—meaning the collection of data abroad. Justice Ginsburg pursued a similar line of questioning, stating, "something has to happen abroad. . . . [T]here are computers in Ireland and something has to happen to those computers in order to get these e-mails back to the United States."

Chief Justice Roberts, on the other hand, signaled during Microsoft's argument that he may consider bifurcating collection from disclosure given that "disclosure takes place in Washington, not in Ireland." Justice Kennedy wondered whether the dichotomy should be rejected in favor of other factors, such as where the owner of the data lives or the service provider's headquarters.

Focusing on technology changes since Congress enacted the SCA, Justices Sotomayor and Ginsburg pointed out that in 1986 Congress could not have anticipated cloud computing technology. Justice Sotomayor noted, "back then they were thinking that where these materials were stored had a geographic existence in the United States, not abroad or [any]where else." She offered that the Court may wish to "leave the status quo as it is and let Congress pass a bill in this new age"; in other words, "if Congress wants to regulate in this brave new world, it should do it." Justice Ginsburg expressed a similar view. Along with Justices Kennedy and Kagan, she lamented the "all or nothing" choices facing the Court.

The Chief Justice challenged the premise of Microsoft's argument, suggesting it would allow parties to protect their e-mail communications from any government intrusion by storing them abroad. Justice Alito picked up on this point, and distinguished between data storage, which "doesn't have a presence anyplace," and "a physical object [that] has a presence someplace."

Amid much discussion of international comity and conflicts with foreign laws, Justice Breyer proposed a "practical solution" that would permit the government to obtain warrants such as the one at issue while allowing the recipient to present objections to a judge, who would perform a comity analysis in order to decide whether the warrant should be enforced.

Global Interest

United States v. Microsoft has attracted substantial international attention, with several countries participating as amicus curiae to express their views on how the case may impact global efforts to regulate cross-border data transfers and data privacy.

In wrestling with how to address cross-border data transfers in cloud storage, for example, the United Kingdom argued against using the location of the storage of data as a determining factor. The United Kingdom suggested that the MLAT process is too slow for modern law enforcement investigations and argued that a territorial approach risked promoting offshore data havens to evade enforcement.

By contrast, New Zealand, the United Nations Special Rapporteur on the Right to Privacy, and the European Community expressed support for a territorial approach, opining that the United States' interpretation of the SCA would be an extraterritorial application of U.S. law and likely would create a conflict for companies trying to comply with U.S. and non-U.S. data privacy laws. The European Commission noted that the

General Data Protection Regulation ("GDPR"), to be implemented this May, requires under Article 48 that court orders requiring data transfers may only be recognized if they are based on international agreements such as MLATs—the procedure the DOJ sought to avoid in this case.

In its brief, the European Commission noted that exceptions to the MLAT requirement exist under the GDPR, such as for transfers "necessary for important reasons of public interest," including combating "serious crime." But exactly how the GDPR will be enforced remains to be seen.

The CLOUD Act

While the parties and the tech and international communities await the Supreme Court's decision, Congress is considering the CLOUD Act. The current bill provides a process for law enforcement to obtain data stored internationally, establishes a means for data hosts to provide data to government officials, and allows hosts to challenge a data request if it is illegal under a foreign country's laws. The passage of the CLOUD Act would clarify the question at issue in Microsoft and could reduce the importance of the Supreme Court's decision going forward.

In February, the CLOUD Act was introduced in both chambers of Congress. Although the bill has not gone through a markup or committee vote, it threatens to render moot the Supreme Court's ruling in *Microsoft*. In its current form, the bill would amend the SCA to establish extraterritorial reach by explicitly stating that it applies to data within a "provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States." The CLOUD Act would further amend the SCA to include a process whereby data providers may challenge an SCA warrant through a motion to quash, and courts would consider any connections to the United States of the subscriber or customer whose data is at issue, as well as principles of international comity.

We continue to track the status of the CLOUD Act and any related legislation.

Conclusion

The Supreme Court will issue a decision in the *Microsoft* case by June. Perhaps before then, Congress will have attempted to resolve the matter through legislation.