Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What To Watch As High Court Takes On Microsoft Warrant Row

By **Allison Grande**

Law360 (February 23, 2018, 10:20 PM EST) -- The U.S. Supreme Court is gearing up to hear arguments Tuesday in a high-stakes fight over the federal government's ability to access data stored abroad by Microsoft, and court watchers expect the justices to focus on a range of thorny legal and public policy issues in their quest to decide the close question of whether privacy rights or law enforcement needs should prevail.

The high court dispute stems from a Second Circuit decision that quashed a warrant issued under the Stored Communications Act, which would have forced Microsoft to produce customer email content data housed on a server located in Ireland. The U.S. Department of Justice, in challenging that ruling, has argued it should be allowed to reach overseas data because this information is controlled by service providers that disclose it to officials within the U.S., while Microsoft has countered that such disclosures constitute an impermissible extraterritorial application of the SCA because the data is physically located abroad.

“The case raises a series of challenging issues — part legal, part legislation and part technology,” said Craig A. Newman, a partner with Patterson Belknap Webb & Tyler LLP and chair of the firm’s data security practice. "And the stakes are high — for law enforcement, cloud storage providers and global privacy rights. It’s clearly one of the most important and most watched privacy cases of the term.”

Here, attorneys offer predictions on how the pivotal oral arguments session is likely to play out.

The Legal Questions

At the heart of the dispute is the Stored Communications Act, a statute that was enacted in 1986 and establishes the rules by which the federal government is allowed to compel third-party service providers to hand over customer data to aid in law enforcement investigations.

The statute is silent about whether the warrants prosecutors obtain under the law can be used to reach digital data stored outside the U.S., setting up the showdown between the government's argument that it's not asking for the warrant to reach abroad because Microsoft controls the data and will turn it over to law enforcement once that information is back at its headquarters in Washington state, and Microsoft's contention that the location of the data — and not the home base of the company that controls it — is what matters most.

“At its core, the appeal focuses on the reach of the Stored Communications Act and the challenging question of where digital data actually lives and the protections that it should be afforded," Newman said.

As they grapple with how to apply a law drafted well before the digital age to a cross-border storage scheme that could not have been envisioned by lawmakers 30 years ago, the justices are likely to have questions for both sides about where the focus of the SCA lies. If the drafters meant for the law to protect users' privacy, as Microsoft argues, then the location of the data would need to be taken into account and the government's reach would be limited to the U.S. But if the purpose of the law is to facilitate information disclosures, as the government asserts, then permitting the government to seize the data once Microsoft brings it back to the U.S. would be allowed.

"The justices are probably going to push on that aspect of the legal arguments, and will likely talk about how the search warrant is different than a subpoena, which under the established law if served on an American company would require it to produce all documents in its possession, control and custody, including records stored overseas," said Hanley Chew, an attorney with Fenwick & West LLP and former federal cybercrime prosecutor.

Microsoft is likely to aim its argument that customers have a reasonable expectation of privacy in communications stored with third-party service providers to the liberal wing of the court, but they could end up finding support for their privacy push from a potential wild card: the newest justice, Neil Gorsuch.

"Justice Gorsuch's confirmation hearing didn't touch on privacy, and that was a big missed opportunity," said Jason Sarfati with Joseph Greenwald & Laake PA.

While traditional conservative thinking tends not to recognize privacy rights that aren't specifically enumerated in a statute, "just because Justice Gorsuch represents the red or right side of the court doesn't necessarily mean he's not on board with privacy rights that aren't written down," according to Sarfati.

Justice Clarence Thomas, who's infamous for his silence at oral arguments, may also be swayed by Microsoft's interpretation of the SCA's intent to protect against improper governmental intrusion on communications held by third parties, given his past endorsement of having a limited government, Sarfati said.

But several justices could also be persuaded by — and are likely to grill the government on — the argument that the user data law enforcement officials are trying to obtain relates to serious crimes like international narcotics trafficking, and restricting access would severely hamper such investigations, attorneys added.

"I don't expect the nine justices to necessarily line up in the traditional liberal and conservative wings, given that multiple movements and desires are playing out all at once," Sarfati said.

The Practical Considerations

During the hourlong arguments session, the justices are expected to go well beyond the pure legal questions surrounding the text of the SCA and delve into more practical aspects of how their ruling will impact both law enforcement's work and tech companies' business models, according to attorneys.

"This is one of those cases where there's a statutory question in front of the justices, and both answers that Microsoft and the government are putting forward have some unappealing implications to them," said David Newman, a national security and data privacy lawyer at Morrison & Foerster LLP. "I would expect to see the justices test each side's theory for how to address these implications and why they should ultimately carry the day in this case."

On the one hand, the government is making the argument that the Second Circuit ruling, if allowed to stand, would impede its ability to quickly and efficiently get the information it needs to solve major, time-sensitive crimes.

While the U.S. government has mutual legal assistance treaties in place with many countries, including Ireland, that would allow it to go through local authorities to obtain the data, prosecutors have argued the process is arduous, time-consuming and unpredictable.

"As a former federal prosecutor, I went through the MLAT process many times, and there were some cases where we never got anything and some cases where it took me years to get any information," said Chew, who added that some of his former colleagues have told him the Second Circuit ruling has already had a significant impact on several ongoing investigations.

Ed McAndrew, a former federal cybercrime prosecutor who now co-chairs the privacy and security group at Ballard Spahr LLP, added that he didn't think the justices would be "impressed" with the argument that the government could get the information through the MLAT process rather than through an SCA warrant, given the way service providers are moving toward breaking up data and storing it in multiple countries.

"If the data is in one country, theoretically you can go through the MLAT process, even though it's impractical in terms of conducting a law enforcement investigation in real time," he said. "But if the content of the account is separated in shards and stored in servers in 70 different countries, then does law enforcement need to file 70 different MLATs?"

The justices could additionally be swayed by the government's argument — which was backed in an amicus brief filed by a bipartisan coalition of nearly three dozen state attorneys general — that the SCA warrants are approved by a judge, while the MLAT process has no similar oversight, Chew said.

"If you look at recent trends, judges have been pushing back on a lot of things, such as saying that gag orders on tech companies can't have an unlimited duration," he said. "I think the justices will recognize that magistrate judges do play a role and aren't just rubber stamps."

On the other side, Microsoft and its supporters — which include the nearly 300 privacy advocates, fellow tech companies, industry groups and lawmakers from 37 countries that signed onto 23 amicus briefs backing the company — have argued that compelling service providers to turn over user data located in other countries would conflict with their legal obligations in foreign countries and sow international discord, with other countries making similar demands for their own investigations.

"I would be surprised if no questions came up at oral arguments in terms of the international privacy concerns, and it will be interesting to see how far the justices will be willing to go in entertaining these considerations," McAndrew said.

The justices are also likely to pose questions that get to how broadly their ruling would sweep. While no other appellate court has ruled on the issue of whether the government can use U.S. law to access data stored abroad, district court judges in California and Pennsylvania have ruled against Google in nearly identical fights to resist such disclosure demands.

The primary distinction between the Microsoft and Google cases appears to be the way the companies have chosen to store the data at issue. While the email account data in the Microsoft case was stored in one place in Ireland, Google breaks up its user data into packets that dynamically move across various servers around the globe, making it difficult to pinpoint a true location for this information.

"The Supreme Court in the Microsoft case could pursue the same line of reasoning as the Second Circuit and say that on this record, the content of an email account stored on a server in Ireland can't be accessed by U.S. law enforcement," McAndrew said. "The reason I don't think the court will do that is because beyond the legal reasons, there's a practical reason that it's not true anymore with most internet service providers that they're using the storage technology at issue in this case."

Given the advancements in cloud computing, a ruling focused solely on the technology at issue in the Microsoft case could end up having little effect on other cases and could be difficult for lower courts to apply to emerging technologies, potentially giving the justices an interest in setting a more broadly applicable rule, attorneys say.

"The court is likely to be reluctant to come up with a rule that rests on technical distinctions and may want to try to find one that is sensitive to different data storage algorithms and practices, although that may be challenging to do," David Newman said.

The Policy Issues

The justices may also address more general policy issues that are outside their mandate but nevertheless can't be ignored in the debate, attorneys say.

Microsoft has argued that if the Supreme Court rules for the government, then other nations will come back to them with legal processes from their own countries demanding user data stored in the U.S. without permission from the U.S. government. While the concern has been raised widely by stakeholders in both the U.S. and EU, court watchers say the justices are more likely to view it as a policy question that Congress needs to resolve.

"For the justices, they may acknowledge that in ruling a certain way they are creating this problem, but will say that it's more of an issue for the U.S. State Department to hash out with the European Union," Sarfati said.

The legal fight has also helped spur movement in Congress to clarify and solidify the ability of law enforcement to access data stored abroad by service providers such as Microsoft.

Earlier this month, a bipartisan coalition of federal lawmakers introduced legislation in both chambers — known as the Clarifying Lawful Overseas Use of Data, or CLOUD, Act — that would give the government a concrete path to enter into formal agreements with foreign nations and set a clear framework for tech companies to comply with such demands.

The proposal joined the International Communications Privacy Act, or ICPA, which has been pending for

several years and would similarly allow law enforcement to obtain from service providers the electronic communications of U.S. citizens and permanent residents regardless of where the individual or communications are located, as long as a warrant is obtained first.

While attorneys say that it's unlikely the justices will delve into the merits of the proposals, their existence could spur the justices to pull back slightly and issue a narrower ruling within the confines of the SCA while acknowledging there is still plenty of room for Congress to act.

"Some of the justice may wrestle with the question of whether this line-drawing that is being done by the court is better done by Congress," David Newman said. "This may be a case where the justices decide one way but raise policy questions that Congress could address."

While the Supreme Court has in other instances given a nod to potential law changes while ruling within the confines of existing laws, some experts noted that given the rapidly changing nature of technology and the current level of congressional gridlock, the justices may be willing to endorse a more broadly applicable standard that would have a more lasting impact.

"The Supreme Court has shown a willingness in recent years to speak a little more broadly when it comes to digital privacy, so it will be interesting to see whether at least some of the justices will be prepared to offer broader pronouncements on these issues," McAndrew said.

Microsoft is represented by E. Joshua Rosenkranz, Robert M. Loeb and Brian P. Goldman of Orrick Herrington & Sutcliffe LLP, James M. Garland and Alexander A. Berengaut of Covington & Burling LLP, Guy Petrillo of Petrillo Klein & Boxer LLP, and in-house attorneys Bradford L. Smith, David M. Howard, John Frank, Jonathan Palmer and Nathaniel Jones.

The federal government is represented by acting Solicitor General Noel J. Francisco, acting Assistant Attorney General John P. Cronan, Deputy Solicitor General Michael R. Dreeben, Assistant to the Solicitor General Morgan L. Goodspeed and Ross B. Goldman of the U.S. Department of Justice.

The case is In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp., case number 17-2, in the U.S. Supreme Court.

--Editing by Pamela Wilkinson and Philip Shea.
