THE RECORDER

Page printed from: *http://www.law.com/therecorder/almID/1202784728964*

Why Google Is Losing the Battle Over Foreign-Stored Data

Despite a legal victory for tech companies last year in the Second Circuit, a series of decisions has gone against Google.

By Ben Hancock | April 27, 2017

(Shutterstock.com)

SAN FRANCISCO — Google Inc. has been on a losing streak in its fight to keep customer data stored on overseas servers out of reach from U.S. law enforcement authorities.

Last week, a federal magistrate judge in San Francisco denied Google's attempt to quash a warrant seeking data stored abroad. It was at least the third such decision involving Google in as many months, and another magistrate judge in Florida in early April forced Yahoo to hand over data in a similar ruling.

The momentum in favor of law enforcement raises questions about whether a landmark decision last year by the U.S. Court of Appeals for the Second Circuit curtailing authorities' power to access

overseas data is in danger of being upset. But it also spotlights the particular challenges faced by Google's approach in waging these courtroom battles.

"It's another example that [the Department of] Justice continues, despite the Second Circuit opinion, to seek access to foreign-stored account data," John Carlin, a partner at Morrison & Foerster and former assistant attorney general of the DOJ's national security division, said of the most recent ruling. "And it is an indication that that litigation strategy might be working."

- Related article: **Google Lawyer Says New Laws Needed to Govern Cloud Data**

Photo: Judge Laurel Beeler, U.S. District Court for the Northern District of California

U.S. Magistrate Judge Laurel Beeler of the Northern District of California, in her order against Google last week, explicitly rejected the reasoning by a panel of Second Circuit judges who in July 2016 denied prosecutors' attempts to access email stored on a Microsoft server in Ireland. A petition for rehearing of that decision en banc was denied in a split decision in January.

Legally speaking, the controversy deals with the application of the Stored Communications Act (SCA), a statute enacted in 1986—long before everyone had email or could envision something called the "cloud"—that allows government access to electronic records with a warrant.

Neither industry nor the Justice Department contests the notion that the law does not apply extraterritorially. But they have been sparring about just what "extraterritorial" means. The Second Circuit panel ruled that accessing the data on Microsoft's Irish server would be an impermissible extraterritorial application of the SCA.

But Beeler noted that regardless of the data being stored overseas, Google admits that the only people able to produce the data are in the United States—specifically, at its headquarters in Mountain View. She therefore ruled that enforcing the warrant would be a "domestic application" of the SCA and not be expanding its scope abroad.

Citing a dissent from the denial of en banc review at the Second Circuit, Beeler added: "'[I]f statutory and constitutional standards are met, it should not matter' where a service provider chooses to store the 1's and 0's."

In broad strokes, that's the reasoning that has been adopted by other magistrate judges as well since the Second Circuit's opinion. On Feb. 3, U.S. Magistrate Judge Thomas Rueter of the Eastern District of Pennsylvania also ordered Google to comply with a warrant seeking overseas data. Google subsequently filed an objection, and U.S. District Judge Juan Sanchez heard arguments on April 18 over whether Rueter's ruling should be reversed.

This could all be a precursor to a fight at the U.S. Supreme Court, even though there isn't yet a true circuit split on the issue. The government on April 12 sought and received an extension of time to file its cert petition of the Second Circuit's decision, with the new deadline set for May 24. It's possibly a signal that the government wants the litigation to percolate further to get more grist for its arguments. Or it may just be because the position of the solicitor general—who makes these kinds of calls—is still vacant.

Critics of the Second Circuit opinion see Google's wave of losses as a sign of the decision's inherent weaknesses. But they also note there are important differences between Microsoft's way of dealing with data and overall legal position, and the approach taken by Google.

Microsoft argued that if authorities in New York wanted the email data in Ireland, all they had to do was go through a treaty process with Irish authorities. By contrast, Google has essentially argued—in part because of its practice of "sharding" data into pieces spread across servers around the globe,

for the purpose of network efficiency—that data stored outside the United States cannot be accessed by U.S. authorities or by authorities in any other jurisdiction. In other words, it's a locked box.

That approach may have painted the company into a corner, said Jennifer Daskal, a professor at American University's Washington College of Law. "When you look at the facts, it's just not tenable to have a situation where no law enforcement authority can access data based on lawful process."

It wasn't always like this. Prior to the Second Circuit's decision, Google routinely complied with warrants for data stored overseas. But especially with other tech industry giants like Microsoft publicly waging a legal campaign couched in notions of consumer privacy, Google appears to loathe to simply continue with the status quo — at least until the legal uncertainty is resolved.

Publicly, the company has advocated strongly for Congress to adopt legislation that would deal with the issue of law enforcement access to overseas cloud data, while stopping short of endorsing a specific solution. No near-term legislative solution appears to be on the horizon for the time being. A Google spokeswoman declined to comment on Beeler's ruling.

For everyday users of services like Gmail, the continuing ambiguity is not exactly heartening either, said Andrew Crocker, a staff attorney at the Electronic Frontier Foundation.

"These cloud services are increasingly central to everyday life," Crocker said. "How and by what rules governments access these data should be clear and should be protective of individuals' rights."