BRACEWELL

INSIGHTS

To Obtain Data Abroad, Government Just Googles It

February 10, 2017

As technology companies expand globally they increasingly are storing customer electronic data in servers outside the United States. To keep apace, the Justice Department has become more creative in adapting existing legal instruments and more persistent in advancing arguments to encourage and in some cases, to compel, companies to turn over customer data stored abroad. While courts, most notably the U.S. Court of Appeals in the Second Circuit in last year's *Microsoft* decision,[1] have resisted government efforts to compel the retrieval and production of electronic information stored overseas, a Pennsylvania federal court has departed from *Microsoft* and ordered Google to disclose internationally stored customer emails.

The Court Breaks from the Second Circuit in *Microsoft*

On February 3, 2017, Magistrate Judge Thomas Rueter held that Google was required to comply with warrants issued pursuant to the Stored Communications Act (SCA) that sought disclosure of emails held in the accounts of two targets of criminal investigations.[2] Google had partially complied with the warrants, but refused to disclose certain user data, relying on *Microsoft* which held that SCA provisions do not apply internationally. Breaking with the Second Circuit, the court applied the principles of more traditional Fourth Amendment jurisprudence to hold that no invasion of customer privacy would occur outside the United States.

In *Microsoft*, the Second Circuit engaged in a close analysis of the SCA's use of the term "warrant," ultimately holding that Congress did not intend for SCA warrants to have a broader – that is, extraterritorial – reach than traditional warrants. The court then moved to the second step of the extraterritoriality analysis, which looks to the focus of the statute and whether there is a permissible domestic application of the statute even if other conduct occurred abroad. The Second Circuit held that the critical invasion of customer privacy occurs when Microsoft accesses the protected content on the overseas server, an impermissible extraterritorial application.

The *Google* court did not dispute the Second Circuit's determination of Congressional intent. Instead, the court departed from *Microsoft*'s holding in the second step of the extraterritoriality analysis after a review of Fourth Amendment jurisprudence, which distinguishes between the possessory interest protected from an illegal seizure and the privacy interest protected from an illegal search. First, the court held that transferring electronic data from an overseas server to a domestic data center is not a seizure that interferes with the customer's possessory interest in the data. The court analogized such a transfer to the movement of paper documents from one place to another or photocopying documents, which are not seizures in Fourth Amendment case law. Next, the court held that the invasion of customer privacy, i.e., the search, occurs when law enforcement reviews the electronic data after the data have been accessed and

disclosed by Google – that is, in Pennsylvania.

In the court's view, key differences between the data at issue in *Microsoft* and in *Google* compelled a different result. In *Microsoft*, the requested user data was housed in a data center in Ireland. A Google user's data, however, is stored in multiple locations; the components of a single user's data might be stored in multiple locations, both within the United States and abroad. Also, Google's storage network automatically shifts data from location to location to maximize efficiency. In other words, although Google is able to retrieve user data whether it is stored domestically, abroad, or both, it is not possible to determine the exact location of a user's data at a given point in time. This uncertainty makes it practically impossible for the government to obtain data through mutual legal assistance treaties, the alternative suggested by the *Microsoft* court.

At bottom, the court concluded that on *Google*'s facts – where the Google account holders were known to reside in the United States, unlike in *Microsoft*, and the alleged illegal conduct also took place here – the SCA, Fourth Amendment precedent, and practical considerations all supported production of the user data rather than allowing Google to shield the data behind ambiguities in location. The court held that Google could not rely on extraterritoriality arguments and granted the government's motions to compel Google to produce the requested data.

Implications for Companies Maintaining Customer Private Data

Google has already announced that it will appeal the decision, so it remains to be seen if the district court will follow the lead of the Second Circuit in *Microsoft* or stake out its own course. The *Google* decision may give companies emboldened by *Microsoft* pause in deciding whether to resist compliance with what they view as overly broad requests for customer data. The different results in the cases, however, may serve as useful guidance for securing data abroad; clearly, with respect to search warrants, there can be value in the ability to precisely identify what data is stored in the United States versus abroad. It may be that Congress will ultimately address the extraterritoriality issue in *Google* and *Microsoft* and clarify the scope of the SCA in a way that provides a clearer path forward for companies.

In the meantime, there is no doubt that technology companies have found themselves on the vanguard of Fourth Amendment law as they are forced to balance the competing needs of cooperation with law enforcement (both legal and strategic) and obligations to protect customer privacy (both legal and commercial). Additionally, technology companies must take into account the practical management of business operations in the face of ever increasing requests for customer data. Google stated that each year it receives an astounding 25,000 pieces of legal process from federal, state, and local government entities seeking disclosure of customer data in criminal matters.

The nature of technology is that it advances and changes. Even if the narrow *Google-Microsoft* issue is resolved, companies will face other ambiguities that cloud their ability to clearly define their privacy policies and protocols. Companies must be nimble in adapting to a changing legal landscape even as they remain committed to their organization's core principles and practical about business realities.

The memorandum of decision is available ***here***. Our more detailed discussion of the *Microsoft* case is ***here***.

[1] In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985 (2d Cir. July 14, 2016).

[2] In re Search Warrant No. 16-960-M-01 to Google, In re Search Warrant No. 16-1061-M to Google, Memorandum of Decision (Feb. 3, 2017).