

INSIGHTS

Pennsylvania District Court Agrees That Google Must Give Up Foreign Server Data

August 29, 2017

On August 17, 2017, a Pennsylvania district court upheld a magistrate judge's order that Google comply with warrants issued pursuant to the Stored Communications Act ("SCA") and produce to the FBI data that was stored, in part, on servers abroad. The decision, written by Judge Juan Sanchez of the Eastern District of Pennsylvania, departs from the Second Circuit's landmark ruling in *Microsoft*¹ by holding that it is the location of the service provider and where it will disclose data that is key to analyzing the extraterritorial reach of the SCA.

In a February decision, U.S. Magistrate Judge Thomas Rueter required that Google comply with SCA warrants and produce the emails of two targets of criminal investigations.² Google contended that the emails were stored in "shards" across multiple locations both within the United States and abroad. In his decision, Magistrate Judge Rueter ruled that extraterritoriality issues were not implicated because the email account user's privacy would not be invaded when Google accesses the data abroad or discloses it, but when law enforcement reviews the electronic data within the United States.

Judge Sanchez agreed with Judge Rueter's ultimate conclusion that requiring Google to produce data stored outside the United States is a domestic application of the SCA. The court reasoned that the focus of the SCA is the circumstances in which the government can require a provider to disclose data, and that the conduct relevant to that focus takes place when the provider makes a disclosure to the government. The court found significant the fact that Google could retrieve and produce the data at issue only from its headquarters in California, where its Legal Investigations Support team is located. In other words, the court determined that the relevant conduct (retrieval and production) occurs within the United States.

The court's interpretation differs markedly from that in *Microsoft*, the Second Circuit decision on which Google relied. There, the Court of Appeals determined that the SCA warrant provision was "protecting the privacy of the content of a user's stored communications" and that the relevant conduct took place when a service provider accessed a customer's protected content. The *Google* court acknowledged this decision, but held that – even were privacy protection the focus of the SCA – the relevant conduct remains the provider's disclosure of data to the government.

While *Microsoft* was widely cheered, by tech companies in particular, at the time it was decided, it is significant that the *Google* court is but the latest – and likely not the last – to break with the Second Circuit. The *Microsoft* decision itself garnered four separate dissents at its rehearing *en banc*, and the *Google* court notes that the analysis in *Microsoft* has been rejected by every magistrate and district court judge that has considered the issue to date.³

For companies that either already store data on servers overseas or are considering doing so, the *Google* decision is instructive. Simply put, a company that can access data – wherever it may be housed – from the United States may be compelled to produce that data in the United States. Unfortunately, however, the *Google* court fails to acknowledge the challenges attendant with producing such data, especially where foreign data privacy regimes might be implicated. As companies make commercial decisions regarding data storage or data sharing with affiliates and partners abroad, it is more critical than ever to be able to identify where company data is stored and what privacy and disclosure requirements are at play.

The *Google* memorandum of decision is available [here](#). Our more detailed discussion of the *Google* case is [here](#) and [here](#).

¹ *In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016), *reh'g en banc denied*, 855 F.3d 53 (2d Cir. 2017).

² *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d 708 (E.D. Pa. Feb. 3, 2017), available [here](#).

³ See *In re Search of Content that Is Stored at Premises Controlled by Google Inc. and as Further Described in Attachment A*, No. 16-mc-80263 (N.D. Cal. Aug. 14, 2017), *aff'g* 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); *In re Search of Info. Associated with [Redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc.*, No. 16-mj-757, 2017 WL 3445634 (D.D.C. July 31, 2017), *aff'g* 2017 WL 2480752 (D.D.C. June 2, 2017); *In re Search of Info. Associated with Accounts Identified as [Redacted]@gmail.com and Others Identified in Attachment A that Are Stored at Premises Controlled by Google Inc.*, No. 16-mj-2197, 2017 WL 3263351 (C.D. Cal. July 13, 2017); *In re Search Warrant to Google, Inc.*, Mag. No. 16-4116, 2017 WL 2985391 (D.N.J. July 10, 2017) (objections filed); *In re Two Email Accounts Stored at Google, Inc.*, No. 17-M-1235, 2017 WL 2838156 (E.D. Wisc. June 30, 2017) (objections filed); *In re Search of Premises Located at [Redacted]@yahoo.com*, No. 17-mj-1238 (M.D. Fla. Apr. 7, 2017); *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d 708 (E.D. Pa. Feb. 3, 2017).