IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN RE SEARCH WARRANT NO. 16-960-M-1 TO GOOGLE	: : :	MJ NO. 16-960
IN RE SEARCH WARRANT NO. 16-1061-M TO GOOGLE	: :	MJ NO. 16-1061

MEMORANDUM

Juan R. Sánchez, J. **August 17, 2017**

Google Inc. seeks review of United States Magistrate Judge Thomas J. Rueter's February 3, 2017, Order granting the government's motions to compel Google to fully comply with two warrants issued pursuant to § 2703 of the Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712. The warrants require Google to disclose to the Federal Bureau of Investigation electronic communications and other records and information associated with four Google accounts belonging to United States citizens in connection with two domestic wire fraud investigations. Google objects to the Order insofar as it requires Google to produce data the company has elected to store on servers located outside of the United States, asserting that enforcing the warrants as to such data would constitute an unlawful extraterritorial application of the SCA, as the Second Circuit Court of Appeals held in *In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016) [hereinafter *Microsoft*], *reh'g en banc denied*, 855 F.3d 53 (2d Cir. 2017) [hereinafter *Microsoft Reh'g*]. Although Google and each of the account holders in question are based in the United States, Google contends it is the physical location of the data to be retrieved—which Google, not the account holder, controls, and which Google can change at any time for its own business purposes—that determines whether the statute is being applied extraterritorially. Because this Court agrees with the government that it is the location of the provider and where it will disclose the data that matter in the extraterritoriality analysis, and because Google can retrieve and produce the outstanding data only in the United States, the Court agrees with the Magistrate Judge's conclusion that fully enforcing the warrants as to the accounts in question constitutes a permissible domestic application of the SCA. The Order granting the government's motions to compel will therefore be affirmed.

BACKGROUND

Google is a United States-based technology company that offers a variety of different online and communications services, including email. *See* Stip. ¶ 1. Although Google's corporate headquarters are located in California, the company stores user data in a number of different locations both within and outside of the United States. *Id.* ¶¶ 1-2. Google operates a "state-of-the-art intelligent network" that automatically moves some types of data, including some of the data at issue in this case, from one network location to another "as frequently as needed to optimize for performance, reliability and other efficiencies." *Id.* ¶ 4. In addition, for some types of data—for example, a Word document attached to an email—the network breaks individual user files into component parts, or "shards," and stores the shards in different network locations in different countries at the same time.[1] *Id.* ¶ 3, Tr. 4. As a result, at any given point in time, data for a particular Google user may be stored not only outside of the country in which the user is located, but in multiple different countries, and the location of the user's data may change at any time based on the needs of the network. *See* Stip. ¶¶ 3-4. Thus, for example, the network

[1] When applied to some types of files, this "sharding" process generates individual shards that are incomprehensible on their own and become comprehensible only when the file is fully reassembled. *See* Oral Arg. Tr. 4-5, Apr. 18, 2017 [hereinafter cited as "Tr. __"] (explaining shards are "not like pieces of a puzzle, where if you got six of the seven pieces, you could make out six-sevenths of the documents"; rather, "[y]ou can't make out anything comprehensible unless you have all seven").

may change the location of data between the time a warrant is sought and the time it is served on Google. *See id.* ¶ 4.

In August 2016, Judge Rueter issued the first of the two warrants in question in this case. The warrant directs Google to provide the FBI with copies of communications and certain other categories of information associated with three Google accounts "stored at premises controlled by Google," and then authorizes the government to seize certain material from the information received. The government sought the warrant as part of an ongoing wire fraud investigation, whose target is both a citizen and resident of the United States, and all three Google accounts to which the warrant pertains belong to citizens and residents of the United States. The victim of the fraud under investigation is likewise located in the United States. In issuing the warrant, Judge Rueter found the government had demonstrated there was probable cause to believe that evidence of the fraud exists in the Google accounts.

Later the same month, United States Magistrate Judge M. Faith Angell issued the second warrant in question, requiring Google to produce to the FBI communications and other records and information associated with a single Google account belonging to the domestic target of a separate wire fraud investigation with a United States-based victim. Like the earlier warrant, this later warrant directs Google to provide the government with copies of certain categories of information associated with the account "located on [Google's] e mail servers" and authorizes the government to seize from Google's production certain files, documents, and communications. In issuing the warrant, Judge Angell found the government had shown there was probable cause to believe the target's Google account contains evidence of the fraud.

Both warrants were directed to Google at its headquarters in California, and Google's responses to the warrants were handled by the company's Legal Investigations Support team in

California. *See* Stip. ¶ 6; Tr. 32. Support team members are the only Google personnel authorized to access the content of user communications in order to produce such materials in response to legal process, and all support team members are located in the United States. *See* Stip. ¶ 5. In response to each warrant, Google searched for and retrieved from its network all responsive information stored at locations in the United States, a process that involves sending a series of queries from Google's headquarters in California to the company's data centers, directing the servers in those data centers to identify, isolate, and retrieve responsive material for Google to produce to the government. *See* Tr. 6-7, 30-31. All of the Google personnel involved in this process are located in California. *See id.* at 32. While Google produced to the government all of the responsive information it confirmed was stored in the United States, it did not produce data not known to be located in the United States. *See* Stip. ¶¶ 7-8. Rather, Google withheld such data based on the *Microsoft* decision in which the Second Circuit held "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." 829 F.3d at 222.[2]

The government thereafter moved to compel Google to fully comply with each warrant, and the matters were consolidated for argument and disposition. On February 3, 2017, Judge Rueter issued a Memorandum of Decision and Order concluding that requiring Google to fully comply with the warrants did not constitute an extraterritorial application of the SCA and granting the government's motions to compel. Google objects to this Order, taking issue with

[2] Prior to the *Microsoft* decision, when responding to a warrant, Google would query its network without regard to where on the network responsive information was located. *See* Tr. 7. Following the *Microsoft* decision, however, Google began limiting its queries to data centers located in the United States. *See id.* at 7-8.

the Magistrate Judge's extraterritoriality analysis. Following briefing of the issue by the parties and amici,[3] this Court held oral argument in this matter on April 18, 2017.

DISCUSSION[4]

The warrants in question were issued pursuant to the SCA, and it is the reach of the SCA's warrant provision that is at issue in this case; hence, the Court's analysis starts with the statute itself. Enacted as part of the Electronic Communications Privacy Act of 1986 (ECPA), the SCA grew out of congressional concern about the lack of privacy protection under existing

[3] Amicus briefs urging the Court to reject the Magistrate Judge's ruling were submitted on behalf of Yahoo, Inc. and on behalf of Microsoft Corporation, Amazon.com, Cisco Systems, Inc., and Apple Inc.

[4] Because these matters were never referred to a magistrate judge by a judge of this court, as contemplated by 28 U.S.C. § 636(b)(1)(A) or (b)(1)(B), the Order granting the government's motions to compel Google's full compliance with the SCA warrants is best understood as an exercise of the Magistrate Judge's jurisdiction under 28 U.S.C. § 636(b)(3), which permits a magistrate judge to be assigned "such additional duties," beyond those that may be assigned under § 636(b)(1)(A) or (b)(1)(B), "as are not inconsistent with the Constitution and laws of the United States." *See 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, at *4 (D.D.C. July 31, 2017). Unlike § 636(b)(1)(A) and (b)(1)(B), § 636(b)(3) does not specify a standard of review. Rather, the applicable standard depends upon whether the matter more closely resembles a pretrial motion that may be referred under § 636(b)(1)(A), in which case it is subject to review under § 636(b)(1)(A)'s "clearly erroneous or contrary to law" standard, or whether it more closely resembles one of the eight categories of motions excepted from § 636(b)(1)(A), in which case it is subject to de novo review under § 636(b)(1)(B). *See NLRB v. Frazier*, 966 F.2d 812, 816 (3d Cir. 1992). In *Frazier*, the Third Circuit Court of Appeals held that a motion to enforce a subpoena to require a witness to testify in a proceeding before an administrative agency was analogous to a dispositive motion and therefore subject to de novo review, *id.* at 817-18, and the case thus provides some support for the conclusion that the de novo standard is applicable here. The Court need not decide the issue, however, as this case turns on a question of law, and even under the clearly erroneous or contrary to law standard, such questions are subject to plenary review. *See Haines v. Liggett Grp. Inc.*, 975 F.2d 81, 91 (3d Cir. 1992) (holding the "contrary to law" standard in § 636(b)(1)(A) "indicates plenary review as to matters of law"); *see also Blunt v. Lower Merion Sch. Dist.*, 767 F.3d 247, 264 n.30 (3d Cir. 2014) (discerning "no difference between the plenary and de novo standards of review").

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**