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

In re Search Warrant No. 16-960-M-01 to Google	:	Misc. No.	16-960-M-01
	:		16-1061-M
In re Search Warrant No. 16-1061-M to Google	:		

MEMORANDUM OF DECISION

THOMAS J. RUETER
United States Magistrate Judge

February 3, 2017

In August, 2016, this court issued two search warrants, pursuant to section 2703 of the Stored Communications Act, 18 U.S.C. §§ 2701 et seq. ("SCA" or "Act"), which required Google Inc. ("Google") to disclose to agents of the Federal Bureau of Investigation ("FBI") certain electronic data held in the accounts of targets in two separate criminal investigations. Each account holder resides in the United States, the crimes they are suspected of committing occurred solely in the United States, and the electronic data at issue was exchanged between persons located in the United States.

Presently before the court are the Government's motions to compel Google to produce electronic data in accordance with these search warrants (the "Motions").[1] Google has partially complied with the warrants by producing data that is within the scope of the warrants that it could confirm is stored on its servers located in the United States. (N.T. 1/12/17 at 13.) Google, however, has refused to produce other data required to be produced by the warrants, relying upon a recent decision of a panel of the United States Court of Appeals for the Second Circuit, Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by

[1] The Government filed a motion to compel in each of the above-referenced cases. See Case No. 16-960-M-01, Doc. 4 and Case No. 16-1061-M, Doc. 5. The motion filed in each case is essentially the same. Accordingly, the court's analysis applies to both motions.

Microsoft Corp., 829 F.3d 197 (2d Cir. 2016) (hereinafter "Microsoft"), rehearing en banc denied, No. 14-2985, 2017 WL 362765 (2d Cir. Jan. 24, 2017).[2] For the reasons set forth below, the court grants the Motions.

I. BACKGROUND

A. Procedural History

On August 2, 2016, the undersigned issued a search warrant pursuant to section 2703(b) of the SCA, for all data associated with three Google accounts held by an individual who resided in the United States (Case No. 16-960-M-01). The Affidavit in support of the Application for the Search Warrant established probable cause that the three Google accounts described therein were being used by the target of the investigation to commit a fraud in violation of federal law. The fraud described in the Application occurred exclusively in the United States and the victim of the fraud was domiciled in the United States. The executed warrant was served upon Google at its offices in California. The warrant directed Google to send the data to an FBI agent in Pennsylvania.

On August 19, 2016, United States Magistrate Judge M. Faith Angell issued a search warrant (Case No. 16-1061-M) to Google for all data associated with an account of an individual who resided in the United States and was a target of an investigation pertaining to the theft of trade secrets from a corporation located in the United States. The Affidavit in support of

---

[2] On a request for a rehearing en banc, the active judges of the Second Circuit were split evenly (four to four) on whether to grant the petition, and thus the petition was denied. The Honorable Susan L. Carney concurred by opinion in the denial of rehearing en banc. No other judge joined in this opinion. Four judges filed separate opinions dissenting from the denial of rehearing en banc. They were the Honorable Dennis Jacobs, Judge José A. Cabranes, Judge Reena Raggi, and Judge Christopher F. Droney. Each dissenting opinion was joined by the other dissenters.

the Application for the Search Warrant established probable cause that the theft occurred in the United States and this conduct violated federal laws. The warrant was served upon Google at its offices in California. The court allowed "Google to make a digital copy of the entire contents of the information subject to seizure." That copy would be provided to an FBI agent located in Pennsylvania. "The contents [would] then be analyzed to identify records and information subject to seizure." See Aff. ¶ 14(I) filed in support of search warrant.

As explained above, Google did not disclose to the Government all of the user data requested in the two warrants. On October 28, 2016, the Government filed a motion to compel Google to comply with the search warrant, filed at Misc. No. 16-960-M-01 (Doc. 4). On October 28, 2016, this court issued an Order to Google to "show cause in a written response by November 14, 2016 as to the basis upon which Google, Inc. chose not to comply with Search Warrant No. 16-960-M-01 (Doc. 4)." On November 22, 2016, Google filed a Response to November 22, 2016 Order to Show Cause and Motion to Amend Non-Disclosure Order (Doc. 7) ("Google Resp."). In its Response, Google argued that it was not required to produce electronic records stored outside the United States. Google also argued that the warrant is "over broad because it does not describe with particularity which services there is probable cause to search." In addition, Google challenged the non-disclosure order entered by this court pursuant to 18 U.S.C. § 2705(b), contending that the order was an "unconstitutional prior restraint on speech." On January 5, 2017, the Government filed a Reply to Google's Response (Doc. 9) ("Gov't Reply").

The procedural history with respect to the Search Warrant at Misc. No. 16-1061-M is similar. On November 22, 2016, the Government filed a motion to compel Google to

comply with the search warrant (Doc. 5). On November 22, 2016, the court ordered Google to "show cause in a written response to be filed by December 22, 2016 as to the basis upon which Google chose not to comply with Search Warrant No. 16-1061-M." On December 22, 2016, Google, Inc. filed its response to the order to show cause and filed a motion to amend the non-disclosure order (Doc. 7). As in its Response filed in 16-960-M-01, Google relied on the Microsoft case to justify its non-compliance and also challenged the non-disclosure order. On January 5, 2017, the Government filed its reply brief in this case (Doc. 8).

By order dated January 6, 2017, the court granted the parties' joint request for consolidation of the two cases for purpose of the oral argument scheduled on January 12, 2017. The parties submitted a Stipulation of Facts, which was filed in both cases on January 12, 2017.[3] At the hearing, both Google and the Government stressed the importance of the issues raised by the Microsoft case. Google explained that each year it receives thousands of requests for the disclosure of user data from federal, state, and local governmental entities in connection with criminal matters. The Government emphasized the critical importance of obtaining the electronic data of criminal suspects residing in the United States. Due to the priority of the issue to both parties, the court will address the questions arising from the Microsoft decision in this Memorandum of Decision, and will separately decide the over-breath and non-disclosure issues in separate orders.

---

[3] The parties entered into a Stipulation regarding the architecture of Google Inc. and its businesses. See Case No. 16-960-M-01, Doc. 22 and Case No. 16-1061-M, Doc. 11.

B. Stored Communications Act

As noted supra, the search warrants at issue in the present cases were issued under section 2703 of the SCA.[4] The SCA "was born from congressional recognition that neither existing federal statutes nor the Fourth Amendment protected against potential intrusions on individual privacy arising from illicit access to stored communications in remote computing operations and large data banks that stored e-mails." In re Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 145 (3d Cir. 2015) (internal quotation omitted), cert. denied (2016). Section 2701 of the Act prohibits unauthorized third parties from, inter alia, obtaining, altering or preventing authorized access to an electronic communication stored in a facility through which an electronic communication service is provided. See 18 U.S.C.§ 2701. Section 2701 also imposes criminal penalties for its violation. Id. Subject to certain exceptions, section 2702 of the Act prohibits providers of electronic communication services and remote computing services from disclosing information associated with and contents of stored communications. See 18 U.S.C. § 2702. Significant to the cases at bar, the SCA also empowers the Government to compel a provider to disclose customer information and records. See 18 U.S.C. §§ 2702(b), 2703. The Government may seek information in three ways: by subpoena, court order, or warrant. See 18 U.S.C. § 2703. The particular method chosen by the Government dictates the showing that must be made by the Government and the type of records that must be disclosed in response.

---

[4] The SCA was passed as part of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

DOCKET ALARM

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.