UNITED STATES DISTRICT COURT EASTERN DISTRICT OF WISCONSIN

Case No. 17-M-1234 (E.D. Wis. Feb. 21, 2017)

⊞ IN RE TWO EMAIL ACCOUNTS STORED AT GOOGLE, INC.

WILLIAM E. DUFFIN U.S. Magistrate Judge

MEMORANDUM AND ORDER

I. Procedural History

On February 13, 2017, the government submitted to this court an application for a warrant pursuant to 18 U.S.C. § 2703 (/statute/18-usc-2703-required-disclosure-of-customer-communications-or-records) asking the court to order Yahoo to disclose email records associated with a particular Yahoo email address. The court finds that the affidavit appended to the application readily establishes probable cause to order Yahoo to disclose the information identified in Attachment B of the affidavit and proposed warrant. However, the warrant asks the court to order Yahoo to disclose "all responsive information—including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of Yahoo."

On February 15, 2017, the government submitted an application asking the court to order Google to disclose email records associated with two particular Gmail email *2 addresses. This application also asks the court to order disclosure without regard to where the data may be stored. As with the affidavit above, the court finds that the affidavit appended to the application readily establishes probable cause to order Google to disclose the information identified in Attachment B of the affidavit and proposed warrant.

II. Relevant Law

Under the Stored Communications Act (SCA) the government may obtain a warrant for "disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system." 18 U.S.C. § 2703(a) (/statute/18-usc-2703-required-disclosure-of-customer-communications-or-records). Translated into simplified terms relevant to the present case, this means that a federal law enforcement officer can ask a United States Magistrate Judge to issue a warrant compelling an email service provider (e.g., Google, Yahoo, Microsoft, etc.) to disclose emails associated with a particular email address. (The statute covers other sorts of information and the relevant application seeks details other than emails, such as account information, but for the sake of simplicity the court will refer here to emails.) If the law enforcement officer demonstrates that there is probable cause to believe that the emails will contain evidence of a crime, the court will order the email service provider to disclose the emails sent from or received at the identified email address. *3

With respect to search warrants generally, under certain circumstances a magistrate judge may issue a warrant authorizing a search in a district other than his or her assigned district. Fed. R. Crim. P. 41(b)(2)-(6). However, aside from narrow exceptions related to searches in a "territory, possession, or commonwealth" of the United States, and properties associated with consular missions, Fed. R. Crim. P. 41(b)(5), Rule 41 is silent as to whether a federal court may issue a warrant for search of property outside of the United States.

III. Relevant Facts

Because the facts presented in the applications relate to ongoing criminal investigations and unexecuted warrants, they will be addressed here in only the broadest terms. For present purposes it is sufficient to state with respect to the application in 17M1234 that investigators learned a person in the United States communicated to an associate through emails sent to and received from the target email address. In the application the affiant identifies the person believed to be in control of the target email address and identifies the European country where that person is believed to reside.

The application assigned case number 17M1235 relates to the further investigation of persons who have already been indicted in this district. There is no indication that the relevant email accounts were used by persons outside the United States. *4

In neither application does that government state that it knows where the data sought might be stored, although both state that it is possible that some of the information sought may be stored on servers located outside of the United States.

IV. *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (/case/microsoft-corp-v-united-states-in-re-a-warrant-to-search-a-certain-endashmail-account-controlled-maintained-by-microsoft-corp) (2d Cir. 2016)

The question of whether a warrant issued pursuant to 18 U.S.C. § 2703 (/statute/18-usc-2703-required-disclosure-of-customer-communications-or-records) may compel an email service provider to disclose emails held on servers outside the United States came to the fore recently in *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (/case/microsoft-corp-v-united-states-in-re-a-warrant-to-search-a-certain-endashmail-account-controlled-maintained-by-microsoft-corp) (2d Cir. 2016). Served with a warrant under the SCA requiring the production of a user's emails, Microsoft determined that some of the information sought was stored at a datacenter in Ireland. *Id.* at 204. Microsoft produced data that was stored in the United States but moved to quash the warrant to the extent it compelled Microsoft to produce content stored on a server located outside the United States. The motion to quash was denied by the magistrate judge who issued the warrant and a district judge. Microsoft appealed to the United States Court of Appeals for the Second Circuit.

The court of appeals noted that, unless Congress explicitly states otherwise, it is presumed that a statute's reach is limited to the borders of the United States. *Id.* at 210 (citing *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247 (/case/morrison-v-national-australia-bank) (2010), and *RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. ___ (/case/rjr-nabisco-inc-v-european-cmty), 136 S. Ct. 2090, 195 L. Ed. 2d 476 (2016)). The court stated that "the SCA is silent as to the reach of the statute as a whole and as to the reach of its *5 warrant provisions in particular." *Id.* at 209. The court conclud-

ed, and the government conceded, that the warrant provisions of the SCA do not contemplate or permit extraterritorial application. *Id.* at 210-16. As such, the issue was whether enforcement of the warrant would constitute an unlawful extraterritorial application of the SCA.

To answer that question, the court set about discerning the "focus" of the SCA. Citing *Morrison*, it stated that "[i]f domestic contacts presented by the case fall within the 'focus' of the statutory provision..., then the application of the provision is not unlawfully extraterritorial." *Id.* at 216. "If the domestic contacts are merely secondary, however, to the statutory 'focus,' then the provision's application to the case is extraterritorial and precluded." *Id.* The court concluded that "the relevant provisions of the SCA focus on protecting the privacy of the content of a user's stored electronic communications." *Id.* at 217. In reaching that conclusion, it rejected the government's argument that the SCA's warrant provisions must be read to focus on "disclosure" of the content rather than on privacy.

Having determined that the "focus" of the SCA is user privacy, the court concluded that execution of the warrant would constitute an unlawful extraterritorial application of the Act. The information sought was the content of electronic communications stored in Ireland. The court expressed its view that "the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government." *6 *Id.* at 220. Because the content would be seized from a datacenter located in Ireland, the conduct that falls within the focus of the SCA would occur outside the United States. *Id.* Thus, to enforce the warrant would constitute an unlawful extraterritorial application of the SCA. *Id.* at 221.

The government sought rehearing en banc. The court divided four to four, thus denying the request. *Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.)*, 2017 U.S. App. LEXIS 1274, 18 (2d Cir. Jan. 24, 2017). Without agreeing that the "focus" of the relevant provisions of the SCA is user privacy, the dissenting judges concluded, in part, that the conduct relevant to the SCA's "focus" is a provider's *disclosure* of emails to third parties, not a provider's *access* to a customer's data. *Id.* at 28. Microsoft's disclosure

of emails to the government would take place at its headquarters in the United States—a domestic application of the SCA. Because enforcement of the warrant involved a domestic application of the SCA, the panel should have affirmed the district court's denial of Microsoft's motion to quash.

V. Analysis

The court finds persuasive the analysis of the four judges dissenting from the denial of en banc rehearing in *Microsoft*. Consistent with their view, the court concludes the relevant section of the SCA is not best regarded as an authorization for law enforcement to seize data but rather as a command for a service provider to disclose *7 data in its possession. If that service provider is subject to the jurisdiction of the court, the court may lawfully order that service provider to disclose, consistent with the SCA, that which it can access and deliver within the United States. "We can conclude that warrants can reach what their recipients can deliver: if the recipient can access a thing here, then it can be delivered here; and if statutory and constitutional standards are met, it should not matter where the ones-and-zeroes are 'stored.'" *Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.)*, 2017 U.S. App. LEXIS 1274, 21 (2d Cir. Jan. 24, 2017). It is immaterial where the service provider chooses to store its customer's data; what matters is the location of the service provider.

In sum, the court does not find that the warrants at issue here implicate extraterritoriality concerns. Although termed a warrant (no doubt partly as a means for reinforcing that these are orders that must be supported by probable cause) the effect of an order under the SCA is to compel the service provider to disclose information in its possession. It is not an authorization for government agents to physically enter any location or to seize anything from either the user or the service provider. As an order compelling action on the part of service provider, what matters is the location of the service provider. Provided the service provider is within the reach of the court, the court may lawfully order that service provider to disclose data in the service provider's custody and control, without regard of where the service provider might choose to store *8 the ones and zeros that comprise the relevant data. Therefore, the court will issue the warrants as requested by the government and order the service providers to disclose all data responsive to the warrant regardless of whether that data may be stored on servers in or outside of the United States.