UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH [REDACTED]@MAC.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.	**Magistrate Case No. 14-228**

MEMORANDUM OPINION

The government challenges an order by Magistrate Judge John M. Facciola denying its second application for a search warrant under § 2703 of the Stored Communications Act, 18 U.S.C. §§ 2701-12. The magistrate judge denied the government's application on the ground that the requested warrant amounted to an unconstitutional general warrant due, in large part, to the procedures set forth in the application for executing the requested warrant. Following the magistrate judge's denial of the search warrant application and the government's subsequent challenge to that decision, the Electronic Frontier Foundation moved for leave to file an amicus brief. Because the government's application complies with the Fourth Amendment and the specific procedures for executing the warrant are permissible under Federal Rule of Criminal Procedure 41 and controlling case law, the magistrate judge's order will be

vacated, and the government's application for a search warrant will be granted.

BACKGROUND

On March 5, 2014, the government filed under 18 U.S.C. § 2703 of the Stored Communications Act, 18 U.S.C. §§ 2701-2712 a sealed application for a search warrant for electronic communications and other evidence stored on a computer.[1] The government's search warrant application related to a specific e-mail account, [redacted]@mac.com, and involved alleged violations of 41 U.S.C. § 8702 (kickbacks) and 18 U.S.C. § 371 (conspiracy). The government's application included an affidavit in support of the search warrant providing factual information to support a finding of probable cause.[2] In addition, the government's application included two attachments that set forth the place to be searched and the particular items

[1] Under the Stored Communications Act, an electronic communications provider is required to disclose contents, records, and other information of an electronic communication to a governmental entity, with or without notice to the subscriber, provided that the statutory requirements are met. 18 U.S.C. § 2703(a), (b), (c)(1)(A). To require an electronic service provider to disclose either the contents of electronic communications, or records and other information, the governmental entity must "obtain[] a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction." Id. § 2703(b)(1)(A), (c)(1)(A).

[2] Due to the government's ongoing criminal investigation, very few details regarding the investigation will be addressed in this opinion.

that the government intended to seize, including specific information that the electronic service provider, Apple, Inc., would be required to disclose. See Govt.'s Application for a Search Warrant ("Govt.'s Application"), Attach. A, Place to Be Searched at 1; Govt.'s Application, Attach. B, Particular Things to Be Seized by the Government at 1. The magistrate judge denied the government's application for a search warrant in part because the application failed to clearly indicate that Apple was required to disclose e-mails in particular, and because probable cause had not been established for all of the emails requested in the search warrant. In Re: Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., Mag. Case No. 14-228 (JMF), 2014 WL 945563, at *2-3 (D.D.C. Mar. 7, 2014). In addition, the magistrate judge objected to the government's use of Rule 41(e)'s "two-step procedure"[3] for gathering evidence whereby Apple would first be required to disclose to the government all e-mails associated with the target e-mail account, and then, at

[3] Federal Criminal Rule 41(e) sets forth the requirements for issuing a warrant, such as the information that must be contained in the warrant and the proper protocol for executing the warrant. Courts are permitted to issue warrants for the "seizure of electronic storage media or the seizure or copying of electronically stored information." Fed. R. Crim. P. 41(e)(2)(B). Included in that provision is authorization for subsequent off-site review of electronic information obtained in accordance with the search warrant. Id. The rule expressly "authorizes a later review of the media or information consistent with the warrant[.]" Id.

a later point, the government would examine the e-mails at separate location to identify evidence specified in Attachment B to the government's application. Id. at *5-6.

The government filed a second application for a search warrant on March 28, 2014. In the revised application, the government indicated that the warrant applied to the e-mail account for "[redacted]@mac.com," and that the warrant covered "information . . . dating from January 14, 2014, to the present, and stored at premises controlled by Apple Inc." Govt.'s Application for a Search Warrant ("Govt.'s 2d. Application"), Attach. A at 1. Attachment B set forth further details on the particular items to be seized, which included the following records:

> All e-mails, including e-mail content, attachments, source and destination addresses, and time and date information, that constitute evidence and instrumentalities of violations of 41 U.S.C § 8702 (Solicitation and Receipt of Kickbacks) and 18 U.S.C. § 371 (Conspiracy), dated between January 14, 2014, to the present, including e-mails referring or relating to a government investigation involving any or all of the following: [individuals and entities have been redacted].

Id., Attach. B at 1. Attachment C to the government's revised application included the specific procedures for executing the search warrant wherein the government would first "conduct a search of the e-mails produced by the Provider and determine which are within the scope of the information to be seized

specified in Attachment B," and then copy and retain those e-mails that are "within the scope of Attachment B." Id., Attach. C at 1. Law enforcement personnel would then "seal any information from Apple that does not fall within the scope of Attachment B," and would be prohibited from "further review [of] the information absent an order of the Court." Id.

The magistrate judge rejected the government's revised application for a search warrant in a second memorandum opinion. In Re: Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., Mag. Case No. 14-228 (JMF), 2014 WL 1377793 (D.D.C. Apr. 7, 2014). Reiterating the rationale set forth in the first memorandum opinion, the magistrate judge again denied the government's application for a search warrant finding that it violated the Fourth Amendment because it amounted to an overly broad search warrant. Id. at *2-3, *5. In addition, the magistrate judge rejected the government's use of the two-step procedure under Rule 41(e), stating that the government was "'abusing the two-step procedure under Rule 41' by requiring Apple to disclose the entire contents of an e-mail account." Id. at *5 (quoting In Re: Search of Info., Mag. Case No. 14-228 (JMF), 2014 WL 945563, at *5). To avoid issuing a general warrant that would permit the government to seize large amounts of data not supported by probable cause, the magistrate judge recommended that Apple

perform the necessary search and turn over any relevant information to the government. Id. at *6.

The government filed a challenge[4] to the magistrate judge's order on April 21, 2014, seeking review of the magistrate judge's decision denying the application for a search warrant. In its challenge, the government argues that the application for search warrant complies with the Fourth Amendment. Govt.'s Resubmission or Appeal from Mag. J.'s Order Denying Application for Search Warrant ("Govt.'s Challenge") at 5-7. In addition, the government argues that the two-step procedure for executing the search warrant is permitted under Federal Rule of Criminal Procedure 41. Id. at 8-13.

On May 2, 2014, the Electronic Frontier Foundation ("EFF") filed a motion for leave to file a brief as amicus curiae in order to address pertinent questions involving the Fourth Amendment and new technologies. Mot. for Leave to File Brief Amicus Curiae of Elec. Frontier Found. at 1.

[4] The government styles its challenge as an appeal, but the reference is a misnomer. With the exception of authority granted by Federal Rule of Criminal Procedure 58 concerning misdemeanor proceedings handled by a magistrate judge under 18 U.S.C. § 3401, the district court does not exercise appellate power. See, e.g., United States v. Choi, 818 F. Supp. 2d 79, 85 (D.D.C. 2011) ("The magistrate judge is not an inferior court, and the district court does not stand in an appellate capacity over the magistrate.").

DISCUSSION

I. STANDARD OF REVIEW

Under the Stored Communications Act, the government may apply for a warrant requiring an electronic service provider to disclose the contents of electronic communications, or other records and information, from a "court of competent jurisdiction." 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). The statute defines a court of competent jurisdiction as "any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that . . . has jurisdiction over the offense being investigated." Id. § 2711(3)(A)(i). Here, the basis for the magistrate judge's jurisdiction is the Federal Magistrates Act, 28 U.S.C. §§ 631-639. The Federal Magistrates Act provides magistrate judges with authority to decide certain pre-trial matters, including whether to grant search warrant applications.[5] Id. § 636(b)(1)(A). A "judge may designate a magistrate judge to hear and determine any pretrial matter pending before the court," provided that the matter does not fall within one of the

[5] Under § 636, pretrial matters include the issuing search warrants. H.R. Rep. 94-1609, at 8, 1976 U.S.C.C.A.N. 6162, 6168; accord Gomez v. United States, 490 U.S. 858, 868 n.16 (1989).

enumerated exceptions set forth in the subsection (b)(1)(A).[6] Id. "A judge of the court may reconsider any pretrial matter under this subparagraph (A) where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law." Id.; see also Gomez, 490 U.S. at 868. Accordingly, the magistrate judge's order denying the government's application for a search warrant under 18 U.S.C. § 2703 will be reviewed to determine whether it is clearly erroneous or contrary to the law.[7]

II. FOURTH AMENDMENT

The Fourth Amendment provides that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. "As the text of the Fourth Amendment indicates, the

---

[6] A "motion for injunctive relief, for judgment on the pleadings, for summary judgment, to dismiss or quash an indictment or information made by the defendant, to suppress evidence in a criminal case, to dismiss or to permit maintenance of a class action, to dismiss for failure to state a claim upon which relief can be granted, and to involuntarily dismiss an action," are not included in this grant of authority to magistrate judges. 28 U.S.C. § 636 (b)(1)(A).

[7] "A finding is clearly erroneous when although there is evidence to support it, the reviewing [body] on the entire evidence is left with the definite and firm conviction that a mistake has been committed." United States v. United States Gypsum Co., 333 U.S. 364, 395 (1948) (internal quotation marks omitted).

ultimate measure of the constitutionality of a governmental search is reasonableness." Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652 (1995) (internal quotation marks omitted). "Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing . . . reasonableness generally requires the obtaining of a judicial warrant." Id. at 653. The Supreme Court has interpreted the Fourth Amendment to require: (1) that the warrant be issued by a neutral magistrate; (2) that the neutral magistrate find that there is probable cause to believe that the evidence sought will "'aid in a particular apprehension or conviction' for a particular offense;" and (3) that the warrant describes with specificity the "'things to be seized,' as well as the place to be searched." Dalia v. United States, 441 U.S. 238, 255 (1979) (quoting Warden v. Hayden, 387 U.S. 294, 307 (1967); Stanford v. Texas, 379 U.S. 476, 485 (1965)).

"A judicial officer who is considering an application for a search warrant must decide 'whether, given all the circumstances set forth in the affidavit before him, including the veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" United States v. Warren, 42 F.3d 647, 652 (D.C. Cir. 1994) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)). "'Under the Fourth Amendment

a search warrant sufficiently describes the place to be searched if the officer with a search warrant can, with reasonable effort ascertain and identify the place intended.'" United States v. Vaughn, 830 F.2d 1185, 1186 (D.C. Cir. 1987) (quoting Moore v. United States, 461 F.2d 1236, 1238 (D.C. Cir. 1972)).

"The manifest purpose of th[e] particularity requirement was to prevent general searches." Maryland v. Garrison, 480 U.S. 79, 84 (1987). General warrants "le[ave] to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched. . . . [These warrants] provide[] no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular home." Steagald v. United States, 451 U.S. 204, 220 (1981). "By limiting the authorization to search to the specific areas and things for which there is probable cause to search," the Supreme Court has explained, "the [particularity] requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." Garrison, 480 U.S. at 84.

A. Application for search warrant

The magistrate judge rejected the government's application as an unconstitutional general warrant not because the government failed to provide sufficient facts to support a

finding of probable cause for the particular e-mails sought, or because the government failed to specify with particularity the electronic records to be seized or the place to search for those records. Rather, in denying the government's application, the magistrate judge determined that the government was attempting to "seize large quantities of e-mails for which it ha[d] not established probable cause." In Re: Search of Info. Associated with [redacted]@mac.com, 2014 WL 1377793, at *5. Moreover, the magistrate judge rejected the government's manner for executing the warrant described in Attachment C to the government's search warrant application. Under those procedures Apple would be required to disclose to the government all e-mails and records related to the [redacted]@mac.com e-mail account. Govt.'s 2d. Application, Attach. C at 1. Upon receiving the relevant e-mails and records, the government would then examine the information obtained to determine what e-mails and other records are specified in the warrant as items to be seized. Id. The magistrate judge determined that because "the two-step procedure is a narrow exception that requires an affirmative showing of need in the warrant application," the government's application was deficient because it "fail[ed] to provide any explanation for why the two-step procedure is necessary." Id. at *5.

However, the government's warrant and the procedures for the warrant's execution appear to comport with the Constitution.

First, the government's search warrant properly restricts law enforcement discretion to determine the location to be searched and the items to be seized. The government identifies the precise location to be searched -- in this case, the [redacted]@mac.com e-mail account -- and specifies in the attachments to its application the particular e-mails to be seized. In this way, law enforcement discretion is constrained and limited to the items to be seized that are specified in Attachment B to the warrant. See generally, Stanford, 379 U.S. at 485-86 ("'The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.'" (quoting Marron v. United States, 275 U.S. 192, 196 (1927)).

Second, the information contained in the affidavit accompanying the search warrant supports a finding of probable cause because there is a fair probability that the electronic communications and records that the government seeks, which are described in detail in the attachments to the government's search warrant application, will be found in the particular place to be searched. Moreover, the affidavit includes additional background information on the particular types of

records that must be disclosed, the specific crimes for which the government seeks evidence, and the targeted entities and individuals. When read together with the affidavit,[8] the government's application provides detailed information of the alleged criminal scheme and a thorough explanation for why evidence relevant to the investigation is likely to be found in e-mail records and other data related to the target email account.

Furthermore, the procedures the government adopts for executing the search warrant comply with the Fourth Amendment and are permissible under Rule 41. "The Federal Rules of Criminal Procedure are carefully tailored ground rules for fair and orderly procedures in administering criminal justice. Rule 41 embodies standards which conform with the requirements of the Fourth Amendment." United States v. Haywood, 464 F.2d 756, 760 (D.C. Cir. 1972). Rule 41 expressly contemplates and authorizes the procedures the government adopts here to execute the search warrant:

[8] The warrant application must be read in conjunction with the affidavit because the warrant application expressly incorporates the affidavit. See, e.g., Vaughn, 830 F.2d at 1186 ("'[T]he warrant may properly be construed with reference to an affidavit for purposes of sustaining the particularity of the premises to be searched, provided (1) the affidavit accompanies the warrant, and in addition (2) the warrant uses suitable words of reference which incorporate the affidavit by reference.'" (quoting Moore, 461 F.2d at 1238)).

> Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.

Fed. R. Crim. P. 41(e)(2) advisory committee's note. Several courts have found the two-step procedure to be reasonable under the Fourth Amendment, provided that there is a valid warrant supported by probable cause.[9] See, e.g., United States v. Schesso, 730 F.3d 1040, 1046 (9th Cir. 2013) (upholding government's seizure of electronic data for a subsequent off-site search where there was a fair probability that evidence would be found on the defendant's personal computer and other electronic devices); United States v. Evers, 669 F.3d 645, 652 (6th Cir. 2012) (6th Cir. 2012) ("The federal courts are in

[9] The D.C. Circuit has not directly addressed the propriety of the procedures for executing search warrants for electronic evidence outlined in Rule 41(e). In its challenge, the government argues that the D.C. Circuit case of United States v. Heldt, 668 F.2d 1238 (D.C. Cir. 1981), "does not reject the two-step process for execution of warrants for electronic evidence." Govt.'s Challenge at 11-12 n.5. Although it is true that the Heldt case does not expressly reject the two-step process under Rule 41, the case is not applicable to the issues presented here -- namely, whether the government may remove all files and records from a location to perform a subsequent search off-site to identify which e-mails are items specified under the search warrant. The Heldt case involved an on-site search performed by law enforcement where certain documents were seized under the plain view exception. That was not a case where, as here, an entire set of files was seized for a subsequent off-site search to identify which items fall within the scope of warrant.

agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a 'sufficient chance of finding some needles in the computer haystack.'" (quoting United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999))).

In addition, because the government's proposed procedures comply with the Fourth Amendment and are authorized by Rule 41, there is no need for Apple to search through e-mails and electronic records related to the target account and determine which e-mails are responsive to the search warrant. Enlisting a service provider to execute the search warrant could also present nettlesome problems. As the government argues persuasively in its challenge, it would be unworkable and impractical to order Apple to cull the e-mails and related records in order to find evidence that is relevant to the government's investigation. Govt.'s Challenge at 17-21. To begin with, non-governmental employees untrained in the details of the criminal investigation likely lack the requisite skills and expertise to determine whether a document is relevant to the criminal investigation. Moreover, requiring the government to train the electronic service provider's employees on the process for identifying information that is responsive to the search

warrant may prove time-consuming, increase the costs of the investigation, and expose the government to potential security breaches.

As the government argues in its challenge, law enforcement officers are provided with considerable discretion in determining how to execute a particular search warrant. Govt.'s Challenge at 7. The Supreme Court has explained that a search warrant's execution is "generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant[.]" Dalia, 441 U.S. at 257. That said, although law enforcement officers are afforded wide discretion in executing search warrants, "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." Id. at 258; see also Zurcher v. Stanford Daily, 436 U.S. 547, 559–60 (1978). Accordingly, the government will be afforded deference in deciding how to execute the search warrant, subject to later review by a court to determine whether the search complied with the Fourth Amendment's reasonableness requirement.

Finally, it should be noted that it is certainly true that searches for electronic data may present increased risks to the individual's right to privacy as technological advances enable law enforcement to monitor and collect large volumes of electronic communications and other data. See, e.g., Schesso,

730 F.3d at 1042 ("Because electronic devices could contain vast quantities of intermingled information, raising the risks inherent in over-seizing data . . . law enforcement and judicial officers must be especially cognizant of privacy risks when drafting and executing search warrants for electronic evidence." (citations omitted)). Discussing the serious risk to privacy in searches involving an individual's personal files, the Supreme Court stated as follows:

> We recognize that there are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. . . . In [these] kinds of searches, responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.

Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976). At the same time, searches for electronic data present unique challenges for law enforcement officials tasked with prosecuting crimes and gathering evidence relevant to criminal investigations. Indeed, the practical realities of searches for electronic records may require the government to examine information outside the scope of the search warrant to determine whether specific information is relevant to the criminal investigation and falls within the scope of the warrant. Given

these competing interests, courts must strike the proper balance between ensuring that the government's ability to effectively and efficiently investigate and prosecute crimes is implemented and assuring respect for individuals' Fourth Amendment rights. See, e.g., United States v. Ganias, No. 12-240-CR, 2014 WL 2722618, *6 (2d Cir. June 17, 2014) ("Because the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools."); United States v. Adjani, 452 F.3d 1140, 1152 (9th Cir. 2006) ("The fact of an increasingly technological world is not lost upon us as we consider the proper balance to strike between protecting an individual's right to privacy and ensuring that the government is able to prosecute suspected criminals effectively."). With these considerations in mind, and for the reasons articulated above, the government's second application for a search warrant will be granted.[10]

[10] The government also asserts that destroying or returning the evidence received from Apple could either expose the government to accusations that it "destroyed exculpatory evidence in violation of Brady v. Maryland," or hinder the government's "ability to lay a foundation for evidence and establish authenticity under Rule 901 and 1001-1006 of the Federal Rules of Evidence." Govt.'s Challenge at 22. The concerns presented by the government are valid and the procedures for executing the search warrant strike the

III. EFF MOTION TO FILE AMICUS BRIEF

Courts have wide discretion in deciding whether to grant a third party leave to file an amicus curiae brief. See Nat'l Ass'n of Home Builders v. U.S. Army Corps of Eng'rs, 519 F. Supp. 2d 89, 93 (D.D.C. 2007). Court have permitted parties to file amicus briefs where "the brief will assist the judges by presenting ideas, arguments, theories, insights, facts, or data that are not to be found in the parties' briefs." Voices for Choices v. Illinois Bell Tel. Co., 339 F.3d 542, 545 (7th Cir. 2003). In addition, courts have granted amici permission to file briefs when "'a party is not represented competently or is not represented at all, when the amicus has an interest in some other case that may be affected by the decision in the present case,'" or in cases where "'the amicus has unique information or perspective that can help the court beyond the help that the lawyers for the parties are able to provide.'" Jin v. Ministry of State Sec'y, 557 F. Supp. 2d 131, 137 (D.D.C. 2008) (quoting Ryan v. Commodity Futures Trading Comm'n, 125 F.3d 1062, 1064 (7th Cir. 1997)).

EFF seeks leave to file an amicus brief in this matter in light of the "critical questions about the application of the Fourth Amendment to emerging technologies," and to address "the

---

appropriate balance between the government's interest in protecting the integrity of its investigation and the privacy interests at stake.

underlying constitutional issues involved here." Mot. for Leave to File Brief of Amicus Curiae of Elec. Frontier Found. at 1-2. Although EFF may be able to offer "arguments, theories, [and] insights," Voices for Choices, 339 F.3d at 545, and other information addressing the Fourth Amendment's application to emerging technologies, such information is addressed in the magistrate judge's comprehensive discussion on the privacy interests at stake in searches for electronic information. See In Re: Search of Info. Associated with [redacted]@mac.com, 2014 WL 1377793, at *3-5. Furthermore, given that the government's application for a search warrant complies with the Fourth Amendment, there is no apparent need to discuss, at least at this stage, the Fourth Amendment's application to various emerging technologies generally. The government's application meets the Fourth Amendment's requirements for issuing a search warrant for electronic evidence and the procedure for executing the warrant is supported by Rule 41. Accordingly, and in light of the wide discretion afforded to courts in determining whether to permit third parties to file amicus briefs, EFF's motion to file an amicus brief will be denied.

CONCLUSION

The government's application for a search warrant complies with the requirements under the Fourth Amendment and the

procedures for executing the warrant are authorized by Rule 41 of the Federal Rules of Criminal Procedure. Accordingly, the magistrate judge's second memorandum opinion and order will be vacated and the government's application for a search warrant will be granted. In addition, EFF's motion to file an amicus brief will be denied. A separate order accompanies this memorandum opinion.

SIGNED this 7th day of August, 2014.

/s/
RICHARD W. ROBERTS
Chief Judge