SUPERIOR COURT OF THE DISTRICT OF COLUMBIA
CRIMINAL DIVISION – SPECIAL PROCEEDINGS

IN THE MATTER OF THE SEARCH OF WWW.DISRUPTJ20.ORG THAT IS STORED AT PREMISES OWNED, MAINTAINED, CONTROLLED, OR OPERATED BY DREAMHOST	**Special Proceedings No. 2017 CSW 003438** **Chief Judge Robert E. Morin**

ORDER

This matter comes before the Court pursuant to the government's Motion to Show Cause seeking to compel DreamHost, LLC ("DreamHost") to comply with a search warrant issued by the Court on July 12, 2017, No. 2017 CSW 3438 (hereinafter, the "Warrant"), and DreamHost's opposition thereto. Upon consideration of the representations and arguments made by the parties in their filed pleadings and during a hearing in this matter on August 24, 2017, the Court ordered parties to submit a proposed order that addressed the search protocols designed to discover data and information pertaining only to those individuals involved in the criminal activity articulated in the July 2017 Warrant, and exclude materials pertaining to innocent third-parties or other illegal activity. Both parties have submitted proposed orders, neither of which contain any explanation regarding how the government will conduct its search without reviewing identifying information of innocent parties associated with the website. At this stage, the Court anticipated the government would have included procedures, or at least a methodology, by which this minimization would occur. Thus, this order further explains the Court's concerns and its direction to the government.

I. Legal Analysis

When a search warrant authorizes the seizure of material protected under the First Amendment, the requirements of the Fourth Amendment must be applied with "scrupulous exactitude." *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978). The First Amendment protects the right to speak and to associate anonymously. *See McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342, 347 (1995); *NAACP v. Alabama*, 357 U.S. 449, 462 (1958). An individual's associational right is protected even where the government does not intend to cause specific harm. *See Lyng v. Int'l Union*, 485 U.S. 360, 367 n.5 (1988). The government must show a compelling interest when it seeks to compel disclosures, such as membership lists, that may indirectly restrict an individual's ability to freely associate. *See NAACP*, 357 U.S. at 463.

Courts have wrestled with how to balance an individual's rights to engage in expressive activity with the government's ability to prosecute criminals, especially where probable cause has been established indicating that a computer, website, or electronic communication(s) contain evidence of a criminal offense. *See, e.g., In re Search of Info. Associated with Fifteen Email Addresses*, 2017 U.S. Dist. LEXIS 117354 (M.D. Ala. July 14, 2017); *In re Search of Info.*, 212 F. Supp. 3d 1023, 1038 (D. Kan. 2016); *In the Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.,* 13 F. Supp. 3d 157, 166 (D.D.C. 2014).

The reality is that electronic evidence of a criminal offense is often intermingled with unrelated data or information, and law enforcement is tasked with locating that criminal evidence amidst all the electronically stored information in a given storage medium. When dealing with the search and seizure of electronic evidence, D.C. Super. Ct. Crim. R. 41 (e)(2) presumptively

authorizes a two-step process by which law enforcement may conduct "a later review of the media or information consistent with the warrant."[1] This rule is analogous and substantially identical to its federal counterpart, Fed. R. Crim. P. 41 (e)(2)(B), as amended in 2009.[2]

Courts have agreed that such a two-step process is appropriate given the practical problems and technical intricacies associated with electronically stored information. *See, e.g., In re A Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@ Gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F. Supp. 3d 386, 392 (S.D.N.Y. 2014) ("In the case of electronic evidence, which typically consists of enormous amounts of undifferentiated information and documents, courts have recognized that a search for documents or files responsive to a warrant cannot possibly be accomplished during an on-site search."); *United States v. Schesso*, 730 F.3d 1040, 1046 (9th Cir. 2013) (upholding the government's seizure of electronic data following subsequent off-site search of defendant's

---

[1] "A warrant under this rule may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in this rule refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." D.C. Super. Ct. Crim. R. 41 (e)(2).

[2] Rule 41 (e)(2)(B) approves a two-step process for the search and seizure of electronically stored information. The Advisory Committee Notes further discuss the need for such a process:

> 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 . . . [E]lectronic 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.

Fed. R. Crim. P. 41 (e) Advisory Committee's Note (2009).

computer and digital storage devices where there was a fair probability of finding evidence on those devices); *United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012) ("The federal courts are in 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)); *Guest v. Leis*, 255 F.3d 325, 334-35 (6th Cir. 2001) (citing cases from the First, Ninth, and Tenth Circuits) ("Because of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers, including their content, was reasonable in these cases to allow police to locate the offending files.").

When reviewing vast amounts of information, it is understood that the government will inevitably come across material that falls outside the scope of the warrant. *See Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) ("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."); *United States v. Sealed Search Warrant*, 2017 U.S. Dist. LEXIS 125792 (N.D. Ala. Aug. 8, 2017) (acknowledging that "some perusal" is generally necessary to determine the "relevance of documents to the crime"). Indeed, "over-seizing" is considered to be an "inherent part of the electronic search process" and oftentimes provides the government with "access to a larger pool of data that it has no probable cause to collect." *In re Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis*, 21 F. Supp. 3d 1, 8 (D.D.C. 2013).

As a result, various courts have stated that, though not required by the Fourth Amendment, additional safeguards on electronic search warrants may be reasonable and appropriate to limit the possibility of abuse by the government. *See, e.g., In re Search of Info.*, 212 F. Supp. 3d at 1038 (acknowledging "that a judge may have the authority to impose reasonable *ex ante* instructions"); *United States v. Christie*, 717 F.3d 1156, 1166-67 (10th Cir. 2013) (discussing that the Fourth Amendment particularity requirement may or may not require limitations *ex ante*); *In re Search Warrant*, 71 A.3d 1158, 1186 (Vt. 2012) (rejecting "any blanket prohibition on *ex ante* search warrant instructions"); *United States v. Hill*, 459 F.3d 966, 976-77 (9th Cir. 2006) ("[W]e look favorably upon the inclusion of a search protocol; but its absence is not fatal."). Notably, the D.C. Circuit has often required the government to implement a search protocol explaining the different tools or methodology that the government will use to conduct its search and how it intends to minimize the risk that data outside the scope of the warrant is discovered. *See, e.g., In re Search of Apple iPhone*, 31 F. Supp. 3d 159, 166 (D.D.C. 2014); *In re Search of Black iPhone 4*, 27 F. Supp. 3d 74, 80 (D.D.C. 2014); *In re Search of ODYS LOOX Plus Tablet*, 28 F. Supp. 3d 40, 46 (D.D.C. 2014); *In re Facebook*, 21 F. Supp. 3d at 11-12.[3]

---

[3] Magistrate Judge Facciola offered a non-exhaustive list of search protocols:

> (1) asking the custodian of the electronically stored information to provide limited information such as e-mails containing certain keywords or sent between particular recipients; (2) appointing a special master to hire an independent vendor to screen the information for relevance and privilege; (3) prohibiting its own computer personnel from disclosing to investigators any information falling outside the scope of the warrant; (4) waiving its reliance upon the plain view doctrine; and (5) using a search protocol designed to reveal only the information for which the government has probable cause to seize.

See 21 F. Supp. at 11-12.

Here, the Court (Judge Wertheim presiding) found probable cause to believe that the website DisruptJ20.org contains evidence of crimes committed in the District of Columbia in violation of D.C. Code § 22-1322 (rioting statute) by individuals for which the Grand Jury has found probable cause to return an indictment. The Warrant does not, and should not, grant carte blanche access to those materials for which the government has not established probable cause. In its execution, the Warrant would allow the government to seize a variety of data and information associated with the website DisruptJ20.org, including email discussion lists and the content of email communications for multiple email accounts that are within the DisruptJ20.org domain. The government may only retain that data and information that evidences the alleged crimes that serve as the basis for the July 2017 Warrant. As the Court highlighted at the hearing, however, because potential evidence is co-mingled with other information, the Warrant in its execution will implicate the privacy and First Amendment rights of website operators and innocent parties who visited or exchanged with the site and engaged in lawful associational and information gathering activity. Because of the potential breadth of the government's review, the Court concludes that it is appropriate to order additional protections based on the First Amendment considerations of innocent third-parties at issue in this case.

II. Optional Minimization Procedures

As a result of its concern, the Court ordered the government to present a minimization plan by which its review of the data and information produced by DreamHost would not include, to the extent possible, data or information of lawful activity not within the scope of the Warrant. While this Court currently declines to rule on any particular procedure or methodology, the government, at the very least, should consider the following minimization "options."[4]

1. General Review:

Prior to any detailed review of the data or information provided by DreamHost to the government, the government may conduct a general review of the data and information to determine the procedures it will employ to minimize the data and information not within the scope of the Warrant (hereinafter "General Review"). During this stage, the government's review will be limited to determining the type of data and information it will seek in its Proposed Detailed Review. The government is not permitted to review individual pieces of data or identifying information at this stage.

In addition, the government should provide the Court with a general methodology or practice it intends to employ to conduct the General Review. Factors to consider in the General Review may include: (i) limiting the review to metadata such as document dates, custodians, filenames, logs, and other non-content information; (ii) identifying the individuals who will be involved in or authorized to conduct this review and who will determine the proposed search protocol(s); (iii) the process for ensuring that the General Review guidelines are followed; and (iv) a general timeline for completion of the General Review.

[4] The government's inclusion or exclusion of any of the following options will not be dispositive of the Court's final order on execution of the Warrant or its acceptance of the government's methodology on the general review and minimization protocol(s).

2. Proposed Detailed Review of Data:

After completing the General Review, the government is required to file a report with the Court explaining (i) the process the government will use to conduct a detailed review of the data and information, (ii) the procedures the government will implement to minimize the review of data and information not within the scope of the Warrant, and (iii) to the extent it can be determined based on the General Review, the government's plan for removing from its possession all data and information not within the scope of the warrant. Each request must also set forth sufficient facts to establish why the sought data or information is relevant to the government's investigation.

In its Proposed Detailed Review, the government must provide sufficient information on the methods that will be used, even if such explanation is technical, to ensure that innocent third-parties' rights are not violated. Search protocols undoubtedly vary in terms of technicality. Yet, it is not unreasonable, especially when core First Amendment rights are at issue, to request the government to provide a methodology or procedure for segregating relevant data and information from that of innocent third parties. For example, the government should describe the phrases and words it will use in keyword searches, or identify specific software and explain how it will be used to identify relevant data and exclude data and information of innocent parties.

The government should also provide the following information: (i) identify the individuals who will be involved in or are authorized to participate in the review of the data and information; (ii) explain what the government will do with the data and information that is initially excluded from the government's review; (iii) clarify the process for ensuring that the authorized individuals will follow the Proposed Detailed Review guidelines; and (iv) provide a timeline for completion of the Proposed Detailed Review.

As indicated at the hearing, the government shall not begin its Proposed Detailed Review of the data and information until such time as this Court provides a final approval of the proposal submitted by the government.

3. Court Approved Review:

The government shall conduct its review of the data in accordance with the plan approved by the Court. Upon completion of the government's Court Approved Review, and having segregated the data and information that the government has identified as within the scope of the Warrant from that data and information determined as outside the scope of the Warrant, the government shall:

(i) file with the Court an itemized list of the data and information that the government believes falls within the scope of the Warrant and the specific reason(s) the government believes that each individual item(s) of data and information falls within the scope of the Warrant;

(ii) permanently remove from its possession any data or information outside the scope of the Warrant; and

(iii) not distribute, publicize, or otherwise make known to any other person or entity, to include any other law enforcement or government entity, the data and information that is outside the scope of the Warrant.

In all stages of the review process, to the extent the government may be required to reveal information that may jeopardize its investigation, it may request the Court to file such information under seal. Sealing will be permitted only where the government has provided sufficient facts to justify the request.

III. Conclusion

The proposed orders do nothing to address the Court's concerns that, absent an appropriate search protocol, the problem that co-mingled data and information produced by DreamHost will improperly violate the privacy and constitutional rights of innocent third parties.

For the reasons stated above, it is this 15th day of September, 2017, hereby SO ORDERED.

Chief Judge Robert E. Morin
Superior Court for the District of Columbia
(Signed in chambers)

Copies to:

Jennifer A. Kerkhoff
John W. Borchert
Assistant United States Attorneys

Raymond 0. Aghaian
Counsel for DreamHost, Inc.