SUPERIOR COURT OF THE DISTRICT OF COLUMBIA
CRIMINAL DIVISION – FELONY BRANCH

IN THE MATTER OF THE SEARCH OF WWW.DISRUPTJ20.ORG THAT IS STORED AT PREMISES OWNED, MAINTAINED, CONTROLLED, OR OPERTED BY DREAMHOST	Special Proceedings Nos. 17 CSW 3438 **HEARING REQUESTED**

UNITED STATES'S MOTION FOR DREAMHOST TO SHOW CAUSE

The United States of America, by and through its attorney, the United States Attorney for the District of Columbia, hereby moves the Court to order DreamHost, Inc. ("DreamHost"), to show cause why DreamHost should not be compelled to comply with a warrant issued by this Court on July 12, 2017, No. 17 CSW 3438, pursuant to 18 U.S.C. § 2703(a), and ordered immediately to provide to the government certain records and information specified within Attachment B to that warrant that are within the possession, custody, or control of Dreamhost, regardless of where such records or information may be stored.

BACKGROUND

On July 12, 2017, this Court authorized a search warrant pursuant to 18 U.S.C. § 2703(a), commanding DreamHost to disclose to the government records and information associated with the website www.disruptj20.org, including communications and content associated with the account. (Ex. A.) That website was used in the development, planning, advertisement, and organization of a violent riot that occurred in Washington, D.C., on January 20, 2017. Attachment A to the warrant identified the particular customer account that is the subject of the warrant, which was www.disruptj20.org. (Ex. A.) Attachment B, Subsection I, of the warrant, titled "Information to be disclosed by Dreamhost," ordered Dreamhost to disclose the following information for that account:

a. all records or other information pertaining to that account or identifier, including all files, databases, and database records stored by DreamHost in relation to that account or identifier;

b. all information in the possession of DreamHost that might identify the subscribers related to those accounts or identifiers, including names, addresses, telephone numbers and other identifiers, e-mail addresses, business information, the length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

c. all records pertaining to the types of service utilized by the user;

d. all records pertaining to communications between DreamHost and any person regarding the account or identifier, including contacts with support services and records of actions taken.

(Ex. A.) Attachment B, Subsection II of the warrant limited the government's seizure to "[a]ll information described above . . . that constitutes fruits, evidence and instrumentalities of violations of D.C. Code § 22-1322[.]"

On Friday, July 14, 2017, the government sent a copy of the Court's search warrant and its attachments to DreamHost by email. (Ex. B.) DreamHost responded that same day acknowledging that it was in receipt of the search warrant but requested that the government personally serve a copy of the Court's search warrant on DreamHost in California. (Ex. B.) On Monday, July 17, 2017, an agent from the Federal Bureau of Investigation personally delivered a copy of the search warrant to DreamHost.[1] (Ex. C.) DreamHost acknowledged being personally served in an email message dated July 18, 2017. (Ex. C.)

[1] The government also sent copies of the Court's search warrant to DreamHost and to DreamHost's registered agent for service of process in California via Federal Express overnight delivery with signature required at delivery. The Federal Express tracking information for each of those packages indicates that they were delivered on July 18, 2017.

On July 19, 2017, the government requested that DreamHost begin an immediate production of materials in response to the Court's search warrant. (Ex. D.) The government also cautioned DreamHost that if DreamHost did not begin to comply with the Court's search warrant, the government may need to seek relief from the Court. (Ex. D.) That same day, the General Counsel for DreamHost replied to the government that DreamHost could not respond to the Court's search warrant at that time because "the entire company" had convened at an "offsite . . . day-long meeting" and "we're all out of the office." (Ex. E.) However, the General Counsel for DreamHost promised that "we will have an update for you (likely tomorrow [July 20]) with production information and instructions." (Ex. E.)

On July 20, 2017, the government again contacted DreamHost to request that the company begin a rolling production of materials responsive to the Court's search warrant. (Ex. F.) Later that day, the government received an email message from Raymond Aghaian, Esq., an attorney representing DreamHost, who requested to have a telephone call with the government to discuss the Court's search warrant. (Ex. F.) Later that day, the government unsuccessfully tried to reach Mr. Aghaian on the telephone to discuss this matter. (Ex. G.) The government also tried to reach Mr. Aghaian—again without success—the next morning, July 21, 2017. (Ex. G.)

On July 21, 2017, the government received an email message from Mr. Aghaian stating four "concerns" with the Court's search warrant:

> 1. There is some uncertainty as to the language in [Attachment B] Section II, paragraph 2, that we would like to clarify and get a better understanding of what exactly is requested. Moreover, we need to be able to inform the subscriber about the warrant, but it is difficult to do so without knowing specifically which accounts or domains are at issue.
>
> 2. The DC Code is very specific about the Superior Court's jurisdictional limit in issuance of search warrants within DC. Since the servers containing the records at issue here are located in

> Portland, Oregon, instead of DC, we would like to ask that you seek the warrants from the appropriate court.
>
> 3. Some of the requested information likely falls under the protected category of information under the Privacy Protection Act and is not subject to search and seizure pursuant to a search warrant;
>
> 4. Some of the information requested appears overbroad, requesting what amounts to all data without any limitations or a specified timeframe, likely constituting an overseizure [*sic*]. For instance, in one of the requests, the warrant seeks the IP addresses of over 1,000,000 visitors to the website.

(Ex. G.) To date, DreamHost has not produced any materials to the government responsive to the Court's search warrant.

ARGUMENT

I. DreamHost has No Legal Basis for Failing to Produce Materials in Response to the Court's Search Warrant

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." A search pursuant to a search warrant is presumed lawful. *Franks v. Delaware*, 438 U.S. 154, 156 (1978). The Court's search warrant in this case is no exception to these legal standards. On July 12, 2017, this Court determined that there was probable cause to believe that "in the premises controlled by DreamHost, Inc., there is now being concealed property, namely stored electronic communications including but not limited to digital files, records, messages, and photographs as set forth more fully in Attachments A and B." (Ex. A.) The Court specified that "[t]his warrant applies to information associated with www.disruptj20.org that is stored at premises owned, maintained, controlled, or operated by DreamHost[.]" (Ex. A, Attach. A.) The Court also specified the types of information that the

Court ordered DreamHost to produce in response to the search warrant. (Ex. A, Attach. B, Section I.) The Court's search warrant further specified that the government could only seize information that constituted "evidence, contraband, instrumentalities, or fruits of violations of D.C. Code § 22-1322." (Ex. A, Attach. B, Section II.) And the search warrant application was itself supported by the sworn affidavit of Detective Greggory Pemberton of the Metropolitan Police Department. D.C. Code § 23-521(a) (a judicial officer may issue a search warrant upon application of a law enforcement officer or prosecutor). Thus, there should be no dispute that the Court's search warrant was properly issued and that DreamHost must comply with the Court's warrant.

DreamHost's suggestion in Mr. Aghaian's July 20 email message that the Court's search warrant runs afoul of "the Superior Court's jurisdictional limits" is misguided. This Court has jurisdiction to issue search warrants requiring the provider of electronic communication services to produce records because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants." 18 U.S.C. § 2711(3)(B). *See* 18 U.S.C. § 2510 (defining "State" to include "the District of Columbia"); 18 U.S.C. § 2711(1) (adopting the definitions of § 2510 for purposes of §§ 2701-2712).

II. DreamHost's Other Objections to Production are without Merit

The other concerns stated in Mr. Aghaian's July 20 email do not afford DreamHost with any justification for refusing to comply with the Court's order. First, DreamHost's claim that there is "uncertainty as to the language . . . of what is requested" in Attachment B, Part II, is wholly irrelevant. That portion of the Court's search warrant sets forth the information to be

seized by the government after DreamHost complies with the Court's order to produce the information described in Attachment B, Part I. Consequently, there is no "uncertainty" with that part of the Court's search warrant that would justify DreamHost in refusing to comply with the warrant.

Second, DreamHost's objection that some of the information that DreamHost must produce pursuant to the Court's order is "protected . . . under the Privacy Protection Act [42 U.S.C. § 2000aa, ("PPA")]," and therefore is "not subject to search and seizure" pursuant to a search warrant also lacks merit. As a factual matter, the Court's search warrant identifies the precise categories of information that DreamHost must provide to the government and precise limitations on the information that the government may seize during its search. (Ex. A, Attach. B.) DreamHost has offered nothing—not even a proffer—to substantiate its concerns that any of the information the Court has required DreamHost to produce would meet the PPA standard of "protected" materials. But even if DreamHost could satisfy that factual threshold, the PPA does not as a factual matter preclude the government from searching and seizing electronic information—even "protected" materials—pursuant to a search warrant. Quite to the contrary, the PPA provides that the exclusive remedy for a person "aggrieved by a search for or seizure of materials in violation of [the PPA]" shall be "a civil cause of action for damages[.]" 42 U.S.C. § 2000aa-6(a). The PPA further provides "[e]vidence otherwise admissible in a proceeding shall not be excluded on the basis of a violation of [the PPA]." 42 U.S.C. § 2000aa-6(e). Thus, DreamHost's "concern" regarding the PPA does not provide DreamHost with a proper basis for refusing to comply with the Court's search warrant.

Third, DreamHost has raised a concern that the Court's search warrant is "overbroad" and may result in an "overseizure [*sic*]." This is simply not a sufficient basis for DreamHost to

refuse to comply with the warrant. The Court has already imposed limitations on the materials that DreamHost is required to produce and on the materials that the government may seize. (Ex. A, Attach. B.) Accordingly, DreamHost's opinion of the breadth of the warrant does not provide it with a basis for refusing to comply with the Court's search warrant and begin an immediate production.[2]

CONCLUSION

For the foregoing reasons, the government asks that the Court issue an order to DreamHost to show cause why DreamHost should not be compelled to comply with the warrant issued by this Court on July 12, 2017, and ordered immediately to provide to the government all of the records and information in Attachment B to the warrant that are within the possession, custody, or control of DreamHost. The government requests that a hearing be schedule in this matter for the week of July 31, 2017.

Respectfully submitted,

CHANNING D. PHILLIPS
UNITED STATES ATTORNEY

By: 

Jennifer Kerkhoff
John W. Borchert (D.C. Bar No. 472824)
Assistant United States Attorneys
United States Attorney's Office for the
District of Columbia
555 Fourth Street, N.W.
Washington, D.C. 20530
(202) 252-7679

July 28, 2017

[2] It is worth nothing that DreamHost has already produced documents to the government in response to a separate request that indicate that the domain name www.disruptj20.org was registered in or about October 2016—less than a year ago.