SUPERIOR COURT OF THE DISTRICT OF COLUMBIA

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. 17 CSW 3438 Chief Judge Robert E. Morin

ORDER

This matter having come before the Court pursuant to the motion to show cause filed by the government seeking to compel DreamHost, LLC ("DreamHost") to comply with a search warrant issued by the Court on July 12, 2017, No. 17 CSW 3438 (hereinafter, the "Warrant"), and upon consideration of the representations and arguments made by the parties in their filed pleadings and during hearings in this matter on August 24, 2017, and September 20, 2017, and consistent with the Court's interim ruling on September 15, 2017, the Court reiterates the following:

As previously observed, courts around the country have acknowledged that, in searches for electronically stored information, evidence of criminal activity will likely be intermingled with communications and other records not within the scope of the search warrant.

Because of the potential breadth of the government's review in this case, the Warrant in its execution may implicate otherwise innocuous and constitutionally protected activity. As the Court has previously stated, while the government has the right to execute its Warrant, it does not have the right to rummage through the information contained on DreamHost's website and discover the identity of, or access communications by, individuals not participating in alleged criminal activity, particularly those persons who were engaging in protected First Amendment activities. The protocols described herein aim to do just that.

Accordingly, the Court deems it appropriate to incorporate procedural safeguards to comply with First Amendment and Fourth Amendment considerations, and to prevent the

government from obtaining any identifying information of innocent persons to the website DisruptJ20.

To ensure that the identities of innocent persons are not revealed, the government must adhere to the following safeguards: (1) file a report with the Court explaining the government's intended search protocol and review procedures designed to minimize access to data and information not covered by the Warrant; (2) if the Court approves the report, the government may only conduct its search on a redacted data set that omits non-subscriber identifying information; (3) upon completion of review, the government must file an itemized list of the materials it seeks to retain with the Court, and explain how such materials are relevant to its investigation and its basis for removing any redactions; and (4) only upon a finding by the Court that the requested information is evidence of criminal activity, as described in the Warrant for which this Court has found probable cause, may the government obtain any un-redacted information, such as the identity of the user.

Accordingly, it is hereby, ORDERED as follows:

1. Pursuant to the Warrant, DreamHost shall produce to the government all information, subject to certain redactions, that is within the possession, custody, or control of DreamHost for the account **www.disruptj20.org** (hereinafter, the "Account"), including any messages, records, files, logs, or information that have been deleted but are still available to DreamHost, or have been preserved pursuant to a request made under 18 U.S.C. § 2703 (f), and meets the following criteria:
    a. For the time period from October 1, 2016, through and including all of January 20, 2017 (Eastern Time), all records or other information, pertaining to the

Account, including all files, databases, and database records stored by DreamHost in relation to that Account;[1]

b. All subscriber information[2] in the possession of DreamHost that might identify the DreamHost subscribers related to the Account, 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; EXCEPT that

e. DreamHost shall not disclose records that constitute HTTP request and error logs;

f. DreamHost shall not disclose the content of any unpublished draft publications (e.g., draft blog posts), including images and metadata that were associated with draft publications;

g. DreamHost shall not disclose the content of any other material or data that constitutes "work product" or "documentary material" that is protected by the Privacy Protection Act ("PPA"); and

---

[1] The information to be provided by DreamHost for the Account shall include the contents of all email accounts with the domain "@disruptj20.org," all "blog" posts, and all electronic mailing lists. However, as referenced further below, DreamHost shall redact any identifying information of all persons—other than DreamHost's subscriber(s)—who communicated with the website until such time as the Court in the exercise of its discretion directs DreamHost to remove any of those redactions.

[2] As described in footnote 8 herein, "subscriber information" does not include the identity of innocent users of the website.

h. DreamHost shall redact the user identifying information of any non-subscriber(s) who communicated through, or interacted with, the website. The identifying information shall include information but is not limited to: names, addresses, email addresses, member and email lists, Internet Protocol addresses from emails sent to the website, information from within the content of any blogs or emails that would identify the individual communicating with the website. DreamHost shall maintain non-redacted versions of all redacted data, because, as set forth below, the Court may subsequently order DreamHost to provide the government with any of those non-redactions.

2. All information provided by DreamHost pursuant to this Order will be produced to the government in formats readable with software tools commonly available to forensic examiners (such as .txt, .tar, native .sql, .xls files) or with software that will be suggested by DreamHost that will allow the government to access the files.

3. To the extent there is material or data that DreamHost believes is protected by the PPA and not subject to disclosure to the government, DreamHost shall prepare a log identifying the type of data (i.e., draft blog post, recording) that DreamHost excludes from the production of material, and shall provide that log to the government without identifying the content of such records.[3]

4. To the extent there is material or data that DreamHost believes is protected by the attorney-client privilege and not subject to government disclosure, DreamHost shall prepare a log identifying the type of communication or data that DreamHost excludes

[3] If the government disputes the application of the PPA to any type of data that DreamHost excludes from its production, the government may seek review with this Court on the issue of whether the type of data falls within the protection of the PPA. The government and DreamHost will file any copies of this log or filings containing information from this log under seal absent further order from the Court.

from the production of material, and shall provide that log to the government without identifying the content of such records.[4]

5. Proposed Search Protocols and Detailed Review of Data

   a. The government has determined that an initial review of only metadata materials provided by DreamHost[5] will not be necessary in light of DreamHost's ability and willingness to redact any indentifying information from materials provided to the government. Accordingly, DreamHost shall produce to the government a redacted data set – i.e., all files responsive to the Warrant that have been redacted by DreamHost to remove all identifying information of any individual(s) who communicated with the website, EXCEPT that

      i. DreamHost shall withhold any responsive record(s) that are subject to the PPA; and

      ii. DreamHost shall withhold any responsive record(s) that are subject to any potential attorney-client privilege.

   b. The government's review will be conducted by a forensic examiner(s) or individual(s) with the U.S. Attorney's Office for the District of Columbia that are named and have been approved by the Court.[6] The prosecutors in this case may

---

[4] If the government disputes the application of the attorney-client privilege designation to any type of data that DreamHost excludes from its production, the government may seek review with this Court on the issue of whether the type of data falls within the protection of the attorney-client privilege.

[5] "[I]t is not necessary for the government to conduct a more limited General Review of only metadata because the search warrant will have been executed in a manner so that the government can conduct its search for evidence of a crime subject to the Court's supervision." Gov't Mem. in Support of Third Proposed Order, at 2.

[6] Because the government's proposed search protocols must comply with the Fourth Amendment and D.C. Super. Ct. Crim. R. 41, and will be approved by the Court, there is no need for DreamHost to

consult with the forensic examiner to determine the Proposed Search Protocols and procedures for the Detailed Review. The government shall store any materials provided by DreamHost in a manner where the data is only accessible to those Court-approved persons conducting the Search Protocols and Detailed Review.

c. The government shall not begin its review of the redacted materials provided by DreamHost until the Court has approved the government's proposal and authorized the government to begin its Detailed Review of the redacted materials. The government must file a report with the Court, *ex parte* and under seal,[7] explaining:

    i. the intended search protocols, such as applying narrowly-defined search terms describing phrases and words designed to minimize the review of data and information not within the scope of the Warrant;

    ii. the process the government will use to conduct its review of the responsive data and information;

    iii. to the extent not already addressed, the procedures the government will implement to minimize its review of data and information not within the scope of the Warrant;

    iv. the government's plan for permanently deleting from its possession all data and information not within the scope of the Warrant;

---

search through e-mails and electronic records to determine which data and information is responsive to the Warrant.

[7] The Court determines that it is appropriate for the government to submit its report *ex parte* and under seal because the government's criminal investigation is ongoing and may be hindered by public disclosure at this time.

v. the individuals who will be involved in or are authorized to participate in the review of the data and information; and

vi. the timeline for completing the Proposed Search Protocols and Detailed Review.

6. Approved Search Protocols and Detailed Review

a. Upon approval by the Court, the government may apply the authorized Search Protocols against the universe of the redacted data set provided by DreamHost.

b. During its review of the redacted data set, and subject to the scope of the Warrant, the government may initially retain all information relating to the development, publishing, advertisement, access, use, administration or maintenance of the Account, including:

i. Files, databases, and database records stored by DreamHost on behalf of the subscriber or user operating the Account, including: (a) HTML, CSS, JavaScript, image files, or other files; (b) SSH, FTP, or Telnet logs showing connections related to the website, and any other transactional information, including records of session times and durations, log files, dates and times of connecting, methods of connecting, and ports; and (c) MySQL, PostgreSQL, or other databases related to the website.

ii. DreamHost subscriber information for the Account, to include: (a) names, physical addresses, telephone numbers and other identifiers, email addresses, and business information; (b) length of service (including start date), types of service utilized, means and source of payment for services (including any credit card or back account number), and billing and payment information; and (c) the date that the domain name disruptj20.org was registered, the registrant information, administrative contact information, the technical contact information and billing contact

used to register the domain and the method of payment tendered to secure and register the Internet domain name.[8]

c. Following the government's review of the redacted data and information, and having identified the data and information that it believes is within the scope of the Warrant, the government shall:

i. file with the Court, *ex parte* and under seal, an itemized list of information that the government believes constitutes evidence of a violation of D.C. Code § 22-1322, and the specific reason(s) why the items sought are relevant to the government's investigation. Evidence of a violation of D.C. Code § 22-1322, as described in the Affidavit in support of the Warrant, includes:

1). evidence concerning the nature, scope, planning, organization, coordination, and carrying out of the above-described offense;

2). communications relating to the planning, organization, coordination, and carrying out of the above-described offense;

3). evidence, including Internet Protocol ("IP") addresses, email addresses, and any other evidence that will help identify individuals who participated in the above-described offense, planned for the above-described offense, organized the above-described offense, or incited the above-described offense; and

4). evidence about the state of mind of individuals who participated in the above-described offense, planned for the above-described

[8] The Court notes that the information sought in paragraph 6(b)(i)-(ii) is generally known as basic subscriber and transactional information for DreamHost subscriber(s), for which the government has already made a sufficient showing of probable cause. This information will not reveal any identifying information of non-subscribers.

offense, organized the above-described offense, or incited the above-described offense.

ii. file with the Court, *ex parte* and under seal, any request(s) for non-redacted identifying information, including an explanation as to why a specific record should be revealed to the government; and

iii. permanently delete from its possession any data or information that does not fall within the authorized scope of the Warrant and separately file under seal, but not *ex parte*, a report identifying how such data is permanently deleted and cannot be restored or recovered.

d. Upon the Court having found probable cause that certain data and information requested by the government is evidence of criminal activity as covered by the Warrant, and that innocent users of the website will not be identified to the government, all such non-redacted data and information shall be provided to the government.

7. The government shall not retain or have any access to any data or information not approved by the Court, absent further Order.[9]

8. The government shall 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 not within the authorized scope of the Warrant.

9. To the extent the government needs a full digital copy of all material provided by DreamHost for purposes of authentication at trial, the government may seek leave of the Court to obtain from the Court the full scope of material disclosed by DreamHost that

[9] The Court denies the government's request to retain any information that constitutes potentially exculpatory evidence because that information is outside the scope of the Warrant, and thus, the government should never have had access to it.

the government is providing to the Court consistent with the procedures set forth in this Order and that the Court will maintain under seal in this case.

SO ORDERED.[10]

Date: October 10, 2017

Chief Judge Robert E. Morin
Superior Court for the District of Columbia

Copies to:

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

Raymond O. Aghaian
Counsel for DreamHost, Inc.

Paul Alan Levy
Counsel for Proposed Interveners

[10] While the Court appreciates the arguments submitted by Does 1through 5, currently it is unknown whether their information will be among those materials ultimately disclosed to the government. Consequently, in the Court's view, Does' claims are not yet ripe. Accordingly, their motions are denied without prejudice. If, however, the government obtains information about Does 1 through 5, it is to notify the Court and the potential intervenors.

Lastly, given the unprecedented level of participation by a service provider, DreamHost, in making suggestions to the Court to ensure that the identities of innocent visitors to the website are protected, the Court will deny any request to stay this Order absent any additional showing.