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

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 a hearing in this matter on August 24, 2017, it is hereby,

ORDERED that, pursuant to that Warrant, DreamHost shall disclose to the government all information 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:

1. **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] AND
2. All information 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

[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.

card or bank account number), and information about any domain name registration; AND

3. All records pertaining to the types of service utilized by the user; AND
4. 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
5. DreamHost shall not disclose records that constitute HTTP request and error logs; AND EXCEPT
6. DreamHost shall not disclose the content of any unpublished draft publications (e.g., draft blog posts), including images and metadata that were associated with draft publications; AND EXCEPT
7. DreamHost shall not disclose the content of any other material or data that is protected by the Privacy Protection Act ("PPA"); AND

IT IS FURTHER ORDERED that all information provided by DreamHost pursuant to this Order will be produced to the government in a format readable with software tools commonly available to forensic examiners (such as .xls files) or with software that will be provided by DreamHost[2]; AND

IT IS FURTHER ORDERED that, 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] AND

IT IS FURTHER ORDERED that, the government may seize all information provided by DreamHost pursuant to this Order that constitutes evidence of a violation of D.C. Code § 22-1322, as

---

[2] The government submits that providing the material in such a format will substantially assist the government in being able to design targeted searches that will limit—if not eliminate entirely—the need for the government to conduct a manual review of content that is outside the Scope of Seizure.

[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.

described in the Affidavit in support of the Warrant, including: (a) evidence concerning the nature, scope, planning, organization, coordination, and carrying out of the above-described offense; (b) communications relating to the planning, organization, coordination, and carrying out of the above-described offense; (c) 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 (d) evidence about the state of mind of individuals who participated (or, knowing about planned violence, refused to participate) in the above-described offense, planned for the above-described offense, organized the above-described offense, or incited the above-described offense (collectively, the "Scope of Seizure"); AND

IT IS FURTHER ORDERED that, so long as it falls within the Scope of Seizure as defined above, the government may seize all information relating to the development, publishing, advertisement, access, use, administration or maintenance of the Account, including:

1. 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;
    c. MySQL, PostgreSQL, or other databases related to the website;
    d. The contents of all e-mail accounts that are within the @disruptj20.org domain (including info@disruptj20.org).
2. 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;

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; AND

IT IS FURTHER ORDERED that upon receipt of the materials provided by DreamHost, the government may conduct a limited General Review of the materials to determine the procedures that the government will use in executing the search of those materials. The government's General Review shall be limited to inspection only of metadata such as document dates, custodians, filenames, logs, and other non-content information. The General Review will be conducted primarily by a forensic examiner with the U.S. Attorney's for the District of Columbia in consultation with other persons whose names will provided to the Court *ex parte* and under seal. The prosecutors on this case may consult with the forensic examiner to determine a Proposed Detailed Review, described further below, which will be submitted to the Court. The forensic examiner will complete the General Review no more than ten business days after receiving the materials provided by DreamHost. The materials provided by DreamHost will be stored in facilities only accessible to the persons conducting the general review.

IT IS FURTHER ORDERED that upon completion of the General Review described above the government shall file a Proposed Detailed Review with the Court *ex parte* and under seal identifying the following: (a) the individuals who will be involved in or are authorized to participate in the review of the data and information; (b) the process the government will use to review the data and information; (c) to the extent not already addressed by that process, the procedures the government will implement to minimize the review of data and information that does not fall within the Scope of Seizure; (d) to the extent it can be determined based on the general review, the government's plan for deleting from its files and servers all data and information that does not fall within the Scope of Seizure following the search and seizure of evidence; (e) the timeline for completing the Proposed Detailed Review; and (f) the steps that the government will take to minimize its review of any information associated with individuals who did not have a criminal purpose in visiting or communicating with the website. The government shall not begin its substantive review of the materials provided by DreamHost until the

Court has approved the Proposed Detailed Review and authorized the government to begin its review. AND

IT IS FURTHER ORDERED that, upon completion of the government's Detailed Review of the data and information provided by DreamHost to the government, and having identified the data and information that is within the Scope of Seizure from that which is outside of the Scope of Seizure, the government shall: (a) file with the Court an itemized list of the data and information that the government believes falls within the Scope of Seizure and the specific reason(s) the government believes that each individual item(s) of data and information falls within the Scope of Seizure; (b) permanently delete from its servers or any other storage medium any data or information that does not fall within the authorized Scope of Seizure; and (c) file with the Court, *ex parte* and under seal, all such data and information, which the government may comply with by filing the full scope of the original material disclosed by DreamHost; AND

IT IS FURTHER ORDERED that, after filing a copy with the Court of the data or information that does not fall within the authorized Scope of Seizure, the government shall not have any access to this data or information without a further Court order; AND

IT IS FURTHER ORDERED that 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 that does not fall within the authorized Scope of Seizure; AND

IT IS FURTHER ORDERED that all data and information that falls within the Scope of Seizure may be copied and retained by the government; AND

IT IS FURTHER ORDERED that, upon completion of the government's review of the data and information provided by DreamHost to the government, the government shall file, *ex parte* and under seal, an itemized list of the data and information that the government has copied and retained as falling within the Scope of Seizure and the reason(s) the government believes that the data and information falls within the Scope of Seizure; AND

IT IS FURTHER ORDERED that, 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 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.

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

Date:

Copies to:

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

Raymond O. Aghaian
Counsel for DreamHost, Inc.