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 Operated by DreamHost	)	**Special Proceeding No. 17 CSW 3438**
	)	**Judge Morin**

DREAMHOST, LLC'S PROPOSED ORDER

Pursuant to the pleadings filed in this matter and the hearings held before Judge Morin on August 24, 2017 and September 20, 2017, and the Court's interim ruling on September 15, 2017, DreamHost LLC hereby submits its proposed order. The proposed order is attached as Exhibit A. Also attached as Exhibit B is a comparison of the proposed order submitted by the government to that submitted by DreamHost.

The Court should accept each of DreamHost's proposed changes to the order.

I. Manner and Methodology of the Minimization Plan

The principal difference between the two proposed orders consist in the manner and methodology of the minimization plan that will dictate what DreamHost will produce to the government and when. Given the core First Amendment interests relating to this distinct matter, the Court has been abundantly clear during the two hearings and in its interim order that: (a) the government is to employ a minimization methodology that would limit the exposure of data that falls outside the scope of the search warrant and (b) the government should not be able to identify the individuals who are either visiting or communicating with the website.

For instance, during the hearing on September 20, 2017, the court specified:

Court: and just to be clear, the general review is not a review of the identity or contents of communication. It's just the metadata.
….

Court: Do you understand that?

Mr. Borchert: I understand that, yes, Your Honor.

(9/20/2017 Hr'g Tr. at 5.)

The Court then went on discussing the identity of the individuals and records falling outside the scope of the search warrant and stated:

Court: The point is people's identities are going to be protected. List of names, identities of write – of email accounts, et cetera, until the Court rules that your, for lack of a better word, search . . . has come up with documents that fall within the warrant. Then when the Court is satisfied that each individual document is covered by the warrant, then the Court will allow you to investigate."

(9/20/2017 Hr'g Tr. at 8.)

Despite the forgoing exchange and clarification, the government's proposed order fails to capture the Court's intent, and in some cases the government has even retracted provisions that were its prior proposal submitted on September 19, 2017, a day before the last hearing. For instance, the government's September 19, 2017 proposed order provided that their General Review would be "limited to inspection only of metadata such as document dates, custodians, filenames, logs, and other non-content information." Yet, the government has now removed that provision entirely from the new proposed order filed after the hearing despite receiving specific instruction from the Court.

Moreover, the government attempts to limit the redaction of information relating to the identity of individuals to "user names" and "email addresses." Based on this approach, while DreamHost could redact the email address of a specific communication, the content in an email or blogpost wherein the sender identifies him or herself would remain available for the government to review.

Accordingly, DreamHost has tried to capture the Court's intent by suggesting a four-step methodology, noted below in a summary fashion, and as outlined in more detail in the proposed order, that would not only protect the identifying information of the individuals, in any form, but would also minimize unnecessarily providing records to the government that are not within the scope of the warrant. A summary outline of this methodology is provided below for ease of reference:

1. General Review
    a. Limited to determining the type of data and information;
    b. DreamHost to initially provide only metadata of records, without any content;
        i. The metadata will consist of underlying information about the files, and not the actual files;
    c. The government will review the metadata to determine the procedures it will use in searching those materials.

2. Proposed Search Protocols to Identify Responsive Data
    a. Upon completing the General Review, the government will identify search protocols, such as search terms, that would be provided to the Court for approval;
    b. Once approved by the Court, the search protocols would be provided to DreamHost for execution against the entire account data set;
    c. DreamHost will provide any records responsive to the search protocols, with the exception of:
        i. Any records subject to the Privacy Protection Act;
        ii. Any records subject to the attorney-client privilege;
        iii. Redact all identifying information of individuals including member and email lists.

3. Proposed Detailed Review of Data
    a. The government will submit to the Court a Proposed Detailed Review plan;
    b. Once approved by the Court, the government will review the responsive records as provided by DreamHost;
    c. The government may seek to seize any records that constitute evidence of a violation of D.C. Code § 22-1322;
    d. Seizure of the records would be contingent upon the government establishing why the record is relevant to the government's investigation;
    e. If the record seized contains redacted identifying information, the government can upon completion of the review request that DreamHost remove the redaction and reveal the identity of the individual in the record.

4. Completion of Review
    a. Upon completion of the review of the responsive records, the government shall segregate data that is within the scope of the warrant from records that are not and file a report with the Court;
    b. The government will permanently delete all records not within the scope of the search warrant and file a separate report identifying how the records were deleted and that they cannot be restored or recovered;
    c. The government will submit an itemized list of all records falling within the scope of the warrant;
    d. The government can at that time request that DreamHost disclose the identity of any individuals redacted in a record that is within the scope of the warrant and appearing on the itemized list;
    e. The government shall not distribute to any other individual, including any other law enforcement or government entity, the records that do not fall within the scope of the warrant.[1]

II. Using *Brady* to Justify Expanding the Scope of the Warrant

DreamHost has deleted the provision from the government's proposed order allowing the government to seize "evidence of any kind that may constitute potentially exculpatory information for any individual." The government cannot justify seizing records falling outside the scope of the search warrant on the basis that it is required to do so to meet its obligations under *Brady*. This would allow the government to simply argue that the absence of evidence of a crime on a particular computer is exculpatory and thus the government must seize the entire computer, even though it would fall outside the scope of the warrant, for the purpose of providing an image of the entire computer to a defendant in case. There would essentially be no limit to what the government can seize when utilizing the two-step process to obtain a vast amount of records.

[1] In relation to the content from multiple unique email accounts utilizing the same domain, which DreamHost submits constitutes an overbroad search, lacks probable cause and is beyond the scope of the warrant, this approach still presents an after the fact justification of the search where the government first reviews records that it has no probable cause to review, and based on what it finds during its review, then justifies the seizure. While not included in the suggested four-step approach above, DreamHost can instead limit execution of the search protocols to records that are not subject to the email accounts. If the government is able to obtain information from its review of the responsive records that do not include content from the email accounts to establish that the multiple email accounts may contain evidence of the underlying crime, it can then obtain a separate search warrant for each specific email account. If it is unable to obtain information from its review of the responsive records to implicate the other email accounts to the criminal activity, then it should not be able to review or possess the content for any of those accounts.

Moreover, the government's obligations under Brady attaches only to "information in the government's *actual* or *constructive possession* that is favorable and material." *Vaughn v. United States*, 93 A.3d 1237, 1244 (D.C. 2014) (emphasis added) (citing *Brady v. Maryland*, 373 U.S. 83, 83 (1963)). While the records falling outside the scope of a warrant are in the government's *temporary* possession when conducting a review of the records under the two-step process, subject to deletion or return once determined that the records are outside the scope of the warrant, they cannot be deemed to be in actual or constructive possession. *See White v. United States*, 763 A.2d 715, 724 (D.C. 2000) ("[a]ctual possession is defined as, 'the ability of an individual to knowingly exercise direct physical custody or control over the [weapon], while constructive possession exists where a person is knowingly in a position or has the right to exercise dominion and control over the [weapon].'"). If the temporary possession in the two-step process constitutes actual or constructive possession, then the entire trove of the information taken as part of the two-step process can itself constitute a seizure and would thus be deemed unconstitutional.

III. As Noted by the Court in its Tentative Ruling on August 24, 2017, the Order Should Include Language Staying the Order Pending an Appeal.

As argued in DreamHost's filing on September 5, 2017, DreamHost continues to include a provision issuing a stay of the order pending appeal. As the Court stated at the conclusion of the hearing on August 24, 2017, "[t]he government won't review it until [DreamHost] make[s] a decision about whether [it is] going to appeal the order." (8/24/2017 Hr'g Tr. at 54-55.) Without repeating the arguments from DreamHost's prior filing on September 5, 2017, the stay provision is appropriate and would constitute irreparable harm if the government were allowed to review the records prior to DreamHost exercising its right to appeal, if it chose to do so.

Therefore, the language in the proposed order should accurately reflect that the government may not review the records until DreamHost has either determined that it will not appeal the order or has otherwise exhausted its right under appeal.

IV. The Court Should Order the Government to Permanently Delete Any Data that Does Not Fall Within the Scope of Seizure and File a Report Explaining How the Deletion Will Occur.

The government has changed the language of its order to provide that the deletion of the records falling outside the scope of the warrant should be deleted *permanently*. Yet, it still refuses to include a provision requiring that it file a report to show that it has done so and that the data deleted cannot be restored. As previously argued by DreamHost in its pleading filed on September 5, 2017, the order should include the proposed language requiring that the government show how the records were deleted permanently.

DATED this 22nd day of September, 2017.

By: /s/ Raymond O. Aghaian
Raymond O. Aghaian
D.C. Bar #478838
Kilpatrick Townsend & Stockton LLP
9720 Wilshire Blvd PH
Beverly Hills, CA 90212-2018
raghaian@kilpatricktownsend.com
(310) 310-7010 office
(310) 388-1198 facsimile
Attorney for DreamHost, LLC

Chris Ghazarian, Esq. (*Pro Hac Vice application submitted)*
DreamHost, LLC
707 Wilshire Blvd., Suite 5050
Los Angeles, CA 90017
chris@dreamhost.com
(213) 787-4401 office
Attorney for DreamHost, LLC

CERTIFICATE OF SERVICE

A true and correct copy of the foregoing was sent via e-mail this 22nd day of September, 2017, to:

AUSA John W. Borchert
U.S. Attorney's Office
555 Fourth Street, N.W.
Washington, D.C. 20530
john.borchert@usdoj.gov

Paul Alan Levy
Public Citizen Litigation Group
1600 20th Street NW
Washington, D.C. 20009
(202) 588-7725
plevy@citizen.org

/s/ Raymond O. Aghaian
Raymond O. Aghaian

EXHIBIT A

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 hearings in this matter on August 24, 2017, and September 20, 2017, it is hereby, ORDERED as follows:

1. 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:

(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 information in the possession of DreamHost that might identify the DreamHost subscribers related to the Account, including names, addresses, telephone numbers 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 the 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.

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

(e) DreamHost shall not disclose records that constitute HTTP request and error logs; and EXCEPT

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

(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 EXCEPT

(h) DreamHost shall redact the identifying information of any individual(s) who communicated with the website. The identifying information can include information such as: names, addresses, emails 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. However, DreamHost shall maintain unredacted versions of all redacted data, because, as set forth below, the Court may subsequently order DreamHost to provide any user name(s) and email address(es) of individuals previously redacted by DreamHost.

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 and native .sql) 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.[2]

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 from the production of material, and shall provide that log to the government without identifying the content of such records.[3]

5. General Review

(a) During this stage, the government's review will be limited to determining the type of data and information the government it will seek in its Proposed Detailed Review. Accordingly, DreamHost will initially provide the government with only metadata of the records in its possession without any content or identifying information of any individuals who communicated with the website. The metadata will consist of the underlying information about the files, rather than the files itself, and may include: file date, file size, file type, content type, the DreamHost user's name that owns the file, and the file name (so long as the file name itself does not include content or identifying information such as "Protest Speech about Trump").

(b) Upon receipt of the metadata materials provided by DreamHost, the government may review the metadata materials to determine the procedures that the government will use in executing the search of those materials. The General Review of the metadata will be

[2] 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.

[3] 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.

conducted primarily by a forensic examiner with the U.S. Attorney's Office for the District of Columbia as well as other persons whose names will be provided to the Court *ex parte* and under seal. The prosecutors on this case may consult with the forensic examiner to determine the procedures for the Proposed Detailed Review, described further below, which will be submitted to the Court for approval before the government engages in any such review.

(c) The government will complete the General Review no more than ten business days after receiving the metadata materials provided by DreamHost. The metadata materials provided by DreamHost will be stored in facilities only accessible to the persons conducting the General Review.

6. Proposed Search Protocols to Identify Responsive Data

(a) Upon completion of the General Review described above, the government shall file a Proposed Detailed Review with the Court under seal identifying search protocols, such as narrowly defined search terms describing the phrases and words, that are to be executed by DreamHost against the universe of the data set in the possession of DreamHost regarding the account at issue herein.

(b) Once the search protocols are approved by the Court, the government will provide the search protocols to DreamHost wherein DreamHost will execute the search protocol(s) and produce any file(s) responsive to the search protocol, EXCEPT

(i) DreamHost shall redact or remove from any file identifying information of any individual(s) who communicated with the website;

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

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

7. Proposed Detailed Review of Data

(a) The government shall not begin its substantive review of the materials responsive to the search protocols provided by DreamHost until the Court has approved the Proposed

Detailed Review and authorized the government to begin a Detailed Review of the responsive materials. 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) to the extent not already addressed, the procedures the government will implement to minimize the review of data and information not within the scope of the Warrant;

(iii) to the extent it can be determined based on the General Review, the government's plan for permanently deleting and removing from its possession all data and information not within the scope of the Warrant;

(iv) the individuals who will be involved in or are authorized to participate in the review of the data and information;

(v) the timeline for completing the Proposed Detailed Review; and

(vi) 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.

(b) During its Detailed Review, 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 described in the Affidavit in support of the Warrant, only if the government can set forth sufficient facts to establish why the sought data or information is relevant to the government's investigation including the basis for which any identifying information redacted within a specific record should be revealed to the government. Evidence of a violation of D.C. Code § 22-1322, as described in the Affidavit in support of the Warrant, includes:

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

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

(iii) 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

(iv) evidence about the state of mind of 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.

(c) During its Detailed Review and subject to the scope of the Warrant, the government may seize 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: (i) HTML, CSS, JavaScript, image files, or other files; (ii) 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; (iii) MySQL, PostgreSQL, or other databases related to the website; and (iv) the contents of all e-mail accounts that are within the @disruptj20.org domain (including info@disruptj20.org).

(ii) DreamHost subscriber information for the Account, to include: (i) names, physical addresses, telephone numbers and other identifiers, email addresses, and business information; (ii) 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 (iii) 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. Completion of Review

(a) 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 the Warrant from that which is outside of 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 delete from its servers or any other storage medium 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; and

(iii) file with the Court, *ex parte*, all such data and information, which the government may comply with by filing the full scope of the original material disclosed by DreamHost. At the time that the government submits its itemized list to the Court, the Government may request that the itemized list be sealed and that the Court order DreamHost to provide any identifying information of individuals previously redacted by DreamHost who communicated with the website.

(b) After filing a copy with the Court of the data or information that does not fall within the authorized scope of the Warrant, the government shall not have any access to this data or information without a further Court order.

(c) 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 the Warrant.

(d) All data and information that falls within the scope of the Warrant may be copied and retained by the government.

(e) 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.

13. This Order is stayed pending the resolution of any appeal of this Order, except that DreamHost is still required to provide the government with the metadata of the records that it is otherwise required to produce under this Order, and that the government is hereby forbidden from reviewing, processing, or otherwise accessing the data and information in any manner during the pendency of the appeal.

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.

EXHIBIT B

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 hearings in this matter on August 24, 2017, and September 20, 2017, it is hereby, ORDERED as follows:

1. 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:

(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 information in the possession of DreamHost that might identify the DreamHost subscribers related to the Account, including names, addresses, telephone numbers 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 the ~~user name(s) and email address(es)~~identifying information of all persons—other than DreamHost's subscriber(s)—who communicated with the website

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

(e) DreamHost shall not disclose records that constitute HTTP request and error logs; and EXCEPT

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

(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 EXCEPT

(h) DreamHost shall redact the ~~user name(s) and email addres(es)~~identifying information of any individual(s) who communicated with the website. The identifying information can include information such as: names, addresses, emails 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. However, DreamHost shall maintain unredacted versions of all redacted data, because, as set forth below, the Court may subsequently order DreamHost to provide any user name(s) and email address(es) of individuals previously redacted by DreamHost.

2. All information provided by DreamHost pursuant to this Order will be produced to the government in ~~a format~~formats readable with software tools commonly available to forensic examiners

---

until such time as the Court in the exercise of its discretion directs DreamHost to remove any of those redactions.

(such as ~~.xls files~~txt, .tar and native .sql) or with software that will be ~~provided~~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.[2]

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 from the production of material, and shall provide that log to the government without identifying the content of such records.[3]

5. General Review

(a) During this stage, the government's review will be limited to determining the type of data and information the government it will seek in its Proposed Detailed Review. Accordingly, DreamHost will initially provide the government with only metadata of the records in its possession without any content or identifying information of any individuals who communicated with the website. The metadata will consist of the underlying information about the files, rather than the files itself, and may include: file date, file size, file type, content type, the DreamHost user's name that owns the file, and the file name (so long as the file name itself does not include content or identifying information such as "Protest Speech about Trump").

(b) Upon receipt of the metadata materials provided by DreamHost, the government may ~~conduct a limited General Review of the~~review the metadata materials to determine the procedures that the government will use in executing the search of those materials. The General

[2] 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.

Review of the metadata will be conducted primarily by a forensic examiner with the U.S. Attorney's Office for the District of Columbia as well as other persons whose names will be provided to the Court *ex parte* and under seal. ~~During this stage, the government's review will be limited to determining the type of data and information the government it will seek in its Proposed Detailed Review.~~ The prosecutors on this case may consult with the forensic examiner to determine the procedures for the Proposed Detailed Review, described further below, which will be submitted to the Court for approval before the government engages in any such review.

(c) The government will complete the General Review no more than ten business days after receiving the metadata materials provided by DreamHost. The metadata materials provided by DreamHost will be stored in facilities only accessible to the persons conducting the General Review.

6. Proposed Search Protocols to Identify Responsive Data

~~5.~~(a) 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:~~ under seal identifying search protocols, such as narrowly defined search terms describing the phrases and words, that are to be executed by DreamHost against the universe of the data set in the possession of DreamHost regarding the account at issue herein.

(b) Once the search protocols are approved by the Court, the government will provide the search protocols to DreamHost wherein DreamHost will execute the search protocol(s) and produce any file(s) responsive to the search protocol, EXCEPT

(i) DreamHost shall redact or remove from any file identifying information of any individual(s) who communicated with the website;

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

---

[3] 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.

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

7. Proposed Detailed Review of Data

(a) The government shall not begin its substantive review of the materials responsive to the search protocols provided by DreamHost until the Court has approved the Proposed Detailed Review and authorized the government to begin a Detailed Review of the responsive materials. The government is required to file a report with the Court explaining:

(~~a) the individuals who will be involved in or are authorized to participate in the review of the data and information; (b~~i) the process the government will use to conduct a detailed review of the data and information;

(~~c~~ii) 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~~scope of ~~Seizure~~the Warrant;

(~~d~~iii) to the extent it can be determined based on the ~~general review~~General Review, the government's plan for permanently deleting and removing from its ~~files and servers~~possession all data and information ~~that does~~ not ~~fall~~ within the ~~Scope~~scope of ~~Seizure following the search and seizure of evidence~~the Warrant;

(iv) the individuals who will be involved in or are authorized to participate in the review of the data and information;

(~~e~~v) the timeline for completing the Proposed Detailed Review; and

(~~f~~vi) 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 a Detailed Review.~~

~~6.~~ (b) During its Detailed Review, 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

described in the Affidavit in support of the Warrant, ~~including~~only if the government can set forth sufficient facts to establish why the sought data or information is relevant to the government's investigation including the basis for which any identifying information redacted within a specific record should be revealed to the government. Evidence of a violation of D.C. Code § 22-1322, as described in the Affidavit in support of the Warrant, includes:

(~~a~~i) evidence concerning the nature, scope, planning, organization, coordination, and carrying out of the above-described offense;

(~~b~~ii) communications relating to the planning, organization, coordination, and carrying out of the above-described offense;

(~~c~~iii) 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)~~ (iv) evidence about the state of mind of 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 (e) evidence of any kind that may constitute potentially exculpatory information for any individual (collectively, the "Scope of Seizure")~~.

~~7.~~(c) During its Detailed Review and subject to the ~~Scope~~scope of ~~Seizure~~the Warrant, the government may seize all information relating to the development, publishing, advertisement, access, use, administration or maintenance of the Account, including:

(~~a~~i) Files, databases, and database records stored by DreamHost on behalf of the subscriber or user operating the Account, including: (i) HTML, CSS, JavaScript, image files, or other files; (ii) 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; (iii) MySQL, PostgreSQL, or other databases related to the website; and (iv) the contents of all e-mail accounts that are within the @disruptj20.org domain (including info@disruptj20.org).

(~~b~~ii) DreamHost subscriber information for the Account, to include: (i) names, physical addresses, telephone numbers and other identifiers, email addresses, and business information; (ii) 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 (iii) 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. Completion of Review

(a) 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~~scope of ~~Seizure~~the Warrant from that which is outside of the ~~Scope~~scope of ~~Seizure~~the Warrant, the government shall:

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

(~~b~~ii) permanently delete from its servers or any other storage medium any data or information that does not fall within the authorized ~~Scope of Seizure~~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; and

(~~c~~iii) file with the Court, *ex parte*, all such data and information, which the government may comply with by filing the full scope of the original material disclosed by DreamHost. At the time that the government submits its itemized list to the Court, the Government may request that the itemized list be sealed and that the Court order DreamHost to provide any ~~user name(s) and email address(es)~~ identifying information of individuals previously redacted by DreamHost who communicated with the website.

~~9.~~ (b) After filing a copy with the Court of the data or information that does not fall within the authorized ~~Scope~~scope of ~~Seizure~~the Warrant, the government shall not have any access to this data or information without a further Court order.

~~10.~~ (c) 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~~scope of ~~Seizure~~the Warrant.

~~11.~~ (d) All data and information that falls within the ~~Scope~~scope of ~~Seizure~~the Warrant may be copied and retained by the government.

~~12.~~ (e) 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.

13. This Order is stayed pending the resolution of any appeal of this Order, except that DreamHost is still required to provide the government with the metadata of the records that it is otherwise required to produce under this Order, and that the government is hereby forbidden from reviewing, processing, or otherwise accessing the data and information in any manner during the pendency of the appeal.

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.