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**
	)	**Chief Judge Morin**
	)	**Hearing: 10:00 a.m. Thurs., Aug. 24, 2017**

NON-PARTY DREAMHOST, LLC'S SUR-REPLY IN OPPOSITION TO (1) UNITED STATES' MOTION FOR DREAMHOST TO SHOW CAUSE AND (2) UNITED STATES' MOTION TO MODIFY ATTACHMENT B OF THE SEARCH WARRANT

I. Introduction

Much has changed since the government filed its motion to compel. DreamHost's opposition to that motion asked the Court to scrutinize the Search Warrant with "particular exactitude" because of the danger it posed to First Amendment interests, and reject it. In its Reply, the government has moved to excise entirely from the Search Warrant: (a) the warrant's unlawful and highly problematic request for data relating to visitors to the website and (b) any unpublished data subject to the Privacy Protection Act. See Exhibit A (consisting of a comparison of the two versions of Attachment B ("Particular Things to be Seized")). The government has also requested that a time limit ending on January 20, 2017 be imposed on the information requested, and, among multiple other proposed changes to Attachment B of the warrant, that a new section be added explaining what the government will do with non-relevant data it collects.

In its Reply, the government alleged they were unaware that DreamHost maintains "emails associated with the Website, including of emails of third parties" as well as "email

discussion lists." (Reply at 14.) While this assertion is inconsistent with the underlying record, nonetheless, the government continues to request this data in its amended request for "all files, databases, and database records." Just as the government previously attempted to identify the visitors to the website, only giving up when challenged, the government continues to attempt to identify those associating with the website by requesting e-mail membership lists and the content of e-mail contacts with the website by third parties.[1] The government does so despite now identifying that it is concerned with a "focused group of people." (Reply at 2.) Even more disturbing, in moving the Court to allow the amendment of the Search Warrant, the government seeks to expand the scope of the Search Warrant by adding several crimes to be covered by the warrant, without a corresponding determination regarding probable cause.

II. Argument

A. The Amended Attachment B Still Lacks Sufficient Particularity

The government alleges that at the time it applied for the Warrant, it was unaware of – and therefore failed to "exclude from the scope of the Warrant" protected subject matter including: 1) emails associated with the Website, including emails of third parties, and 2) membership lists for email discussion lists, from email accounts sponsored by the website. (Reply at 14 (quotations omitted); see also Opp'n at 8.) Although the government now claims it no longer seeks such materials, however, the revised Warrant requires DreamHost to produce these materials, which are included among "all records or other information, pertaining to [www.disruptj20.org], including all files, databases, and database records stored

[1] The government's reply brief inserts a 28-line single spaced footnote in an effort to continue to justify its initial request for the overbroad set of data that they have now withdrawn. Buried in this footnote, the government still argues that the now withdrawn Attachment B was "nonetheless lawful and appropriate."

by DreamHost in relation to that Account."[2] (Reply Ex. 3 at Part I.a.) While the government identifies in its Reply brief that its concern relates to "a focused group of people" and "closely-held meetings that were not open to the media or public," (Reply at 2), it continues to attempt to obtain information about membership lists from email discussion lists and identify third parties and political dissidents by reviewing the emails submitted to the website for information to accounts such as info@disruptj20.org. Moreover, despite knowing that there were several individual email accounts each with separate login and password requirements, the government attempts to access and obtain content from multiple email accounts with the use of a single search warrant.

The revised Warrant broadly allows the government to obtain such materials as part of "[t]he contents of e-mail accounts that are within the @disruptj20.org domain (including info@disruptj20.org)," with no limitation whatsoever to particular email accounts or addresses. Id. Part II.B. Disclosure of such email content and addresses would reveal the identities of any third parties that exchanged emails with the website. This seizure unjustifiably infringes upon protected First Amendment associational and expressive rights, and lacks sufficient particularity to avoid infringing upon these rights.

As reiterated last week by the D.C. Circuit in United States v. Griffith, to comply with the Fourth Amendment, a search warrant must describe each item to be seized with particularity. United States v. Griffith, No. 13-3061, 2017 WL 3568288, at *7 (D.C. Cir. Aug. 18, 2017) ("In obligating officers to describe the items to be seized with particularity, the Fourth Amendment prevents 'the issu[ance] of warrants on loose, vague or doubtful

[2] In contrast, after acknowledging it was not seeking website visitors after the riot, or draft blog posts, the government excluded these materials from production. (See Reply at 14, Ex. 3 at Part I.a, e.)

bases of fact.'") (quoting Go-Bart Importing Co. v. United States, 282 U.S. 344, 357 (1931)). In Griffith, the Court addressed a search warrant authorizing police to seize "all electronic devices" from the apartment of Griffith, who was a suspected getaway driver in a homicide. The Court held that this search warrant was overbroad because it "broadly authorized seizure of all cell phones and electronic devices, without regard to ownership" because there was no probable cause to seize each and every device in the suspect's apartment. Griffith, 2017 WL 3568288, at *8. The Court explained that "[t]he warrant's overbreadth is particularly notable because police sought to seize otherwise lawful objects," noting, for example, that the suspect shared the apartment with his girlfriend, and that the warrant therefore improperly "authorized police to search for and seize all of her electronic devices." Id. The Court further explained that "[i]n this case, the warrant should have limited the scope of permissible seizure to devices owned by Griffith, or devices linked to the shooting." Id.

Here, the government's attempt to obtain all "contents of e-mail accounts that are within the @disruptj20.org domain" fails to satisfy the particularity requirement. Each email address is associated with a separate user, with a separate login and password. (Opp'n at 8, Fry Decl. at ¶3.) The government, however, has not contended that any of these specific email addresses belong to any persons who had any involvement in the January 20th riot. In fact, the only specific email address that the government identifies, info@disruptj20.org, appears to be the general informational email address for the website, and the government has not contended that this email address belongs to any person involved in the January 20th riot.[3] Therefore, the warrant improperly seeks to obtain email account contents, which are

[3] Nor may the government rely on the affidavit submitted in support of the search warrant to satisfy particularity, since the Search Warrant fails to incorporate the affidavit. See Griffith, 2017 WL 3568288, at *9 ("We read

"otherwise lawful" or "innocuous objects." Griffith, 2017 WL 3568288, at *8 (citation omitted).

Furthermore, the overbroad nature of the Warrant endangers the First Amendment rights of not only the account holders not part of the government's "focus[] group", but the third parties they communicated with.

See Zurcher v. Stanford Daily, 436 U.S. 547, 565 (1978) ("[C]ourts apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search."). Allowing the government to identify the emails and communications with the third parties, that appear to fall outside the government's "focus[] group," endangers the First Amendment associational rights of anyone falling outside this "focus[] group." "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." See NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958). Likewise, by allowing the government to identify previously anonymous individuals, the Warrant endangers the First Amendment rights to engage in anonymous expressive activity, and to read information free from the surveillance of the government. See McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 347, 357 (1995) (reiterating that the right to engage in anonymous expressive activities is critical to adequate protection of underlying speech rights); Stanley v. Georgia, 394 U.S. 557, 565 (1969) ("If the First Amendment means anything, it means that a State has no business telling a man . . . what books he may read or what films he may watch."). While, the government argues that it did not intend to use the

---

warrants by reference to an affidavit… only if the issuing judge uses 'explicit words on the warrant' indicating an intention to incorporate the affidavit's contents and 'thereby limit [the warrant's] scope.'") (quoting United States v. Maxwell, 920 F.2d 1028, 1032 (D.C. Cir. 1990)).

Warrant to "chill free association and the right to free speech," (Reply at 3) the government fails to acknowledge that the mere act of seizing website visitor information (such as HTTP logs and email addresses) will itself have a chilling effect on individuals' associational freedoms guaranteed by the Constitution. Causing an individual to second guess his or her political expression while visiting legal Internet websites for fear of being exposed directly interferes with their associational rights.

Accordingly, to protect lawful content protected by the First Amendment, the Court should not permit the government to obtain electronic information that would trample upon the privacy of non "focus[] group" email account holders as well as third parties.

B. The Government Cannot Broaden the Search Warrant After It Has Been Issued

The central premise of the government's Reply – that the flaws in the Search Warrant pointed out by DreamHost can be fixed by substituting an "amended" Attachment B for the original Attachment B over six weeks after the Search Warrant was issued – is totally unworkable. At the heart of any search warrant is the finding by the judge issuing the warrant that there is probable cause to believe that the property identified by law enforcement is evidence of a specific offense or offenses. See D.C. Code § 23-521(d). In the case of the Search Warrant, Senior Superior Court Judge Werthheim was "satisfied" that the property identified by Detective Pemberton in the original Attachments A and B was subject to seizure as evidence of a violation of D.C.'s rioting statute, D.C. Code § 22-1322. See D.C. Superior Court Search Warrant dated July 12, 2017, attached as Exhibit A to the United States' Motion for DreamHost to Show Cause ("Search Warrant"). Consistent with Senior Judge Wertheim's probable cause decision, the original Attachment B to the Search

Warrant described the information to be seized as information constituting "fruits, evidence and instrumentalities of violations of D.C. Code §22-1322 . . . ." See id.

Among other changes, the government's amended Attachment B now broadens the description of the information to be seized to include evidence of two additional crimes – violations of D.C. Code § 22-1805a (Conspiracy to commit crime) and D.C. Code § 303 (Malicious burning, destruction, or injury of another's property). In doing so, the government has significantly altered the nature of the warrant it applied for, and therefore the information on which Senior Judge Wertheim based his probable cause determination. The government has provided no authority for the proposition that it can seek to broaden a search warrant without a new probable cause determination and under a new sworn affidavit.

C. The Government Has Not Demonstrated that D.C. Law Authorizes Extraterritorial Search Warrants

In its Reply, the government continues to assert that the Stored Communications Act is a "grant of authority" to the District of Columbia to issue a search warrant to an electronic communication service located outside of D.C. (Reply at 6.) As DreamHost pointed out in its Opposition, that conclusion has been repeatedly rejected by state appellate courts carefully considering the issue. The Rose and AT&T cases cited by DreamHost demonstrate that, while the SCA by its terms grants extraterritorial jurisdiction to federal courts with "jurisdiction over the offense being investigated," the SCA contains no equivalent grant to the courts of the states and the District of Columbia.[4]

[4] The government attempts to use Rose and AT&T to its advantage by pointing out that the ultimate result in both cases was to permit extraterritorial warrants. (See Reply at 7.) But, as DreamHost demonstrated in its Opposition, the statutory schemes of Oregon and New Hampshire are easily distinguishable, either because state law expressly allowed out-of-state warrants (Oregon) or was silent on the issue (New Hampshire). The District of Columbia law is neither silent nor allows such out-of-state warrants. Instead, the law in the District of Columbia expressly limits the jurisdiction of the Court.

As the government acknowledges, the D.C. Code and Rules of Criminal Procedure both allow search warrants carried out within the District only. The D.C. Code speaks of "a search to be conducted" in the District of Columbia," D.C. Code § 23-521, and Rule of Criminal Procedure 41(f)(2) refers to a search warrant "executed" within the District. D.C. Super. Ct. R. Crim. P. 41(f)(2). The government tries to avoid these plain territorial limits on search warrants by arguing that the Search Warrant was in fact "executed" within D.C., and authorizes a search that will be conducted in D.C.

The government cites one case for this novel meaning of the term "executed" and definition of "search" – last month's D.C. federal court decision concerning Gmail. In re Search of Info. Associated with [redactedJ@gmail.com that is Stored at Premises Controlled by Google Inc. ("Google"), 2017 WL 344634 (D.D.C. July 31, 2017). It should be noted at the outset that the Google case dealt with the issue of whether a federal court could compel the production of data kept overseas, a question very different from the one presented here, especially because, as discussed previously, the SCA treats federal courts and state courts very differently where extraterritorial jurisdiction is concerned. More to the point, the Google court did not conclude that a search warrant issued pursuant to the SCA should be considered to have been executed in its place of origin. Instead, the court noted, quoting a law review article, that "[SCA warrants] are 'executed' when a law enforcement agent delivers (sometimes by fax) the warrant to the [service provider]." Google, 2017 WL 3445634 at *18 (emphasis added). With this understanding, the Search Warrant should be

considered to have been executed in California, where it was delivered to DreamHost.[5] Because it was executed in California, the Search Warrant does not comport with D.C. law.

The government's suggestion that the recent Google case shows that no "search" occurs until the data is reviewed by government agents is also without merit. The lengthy passage from the opinion quoted by the government stands only for the proposition that Google's internal movement of data does not constitute a search. However, the very passage quoted by the government states that "[a] search occurs when an expectation of privacy that society is prepared to consider reasonable is infringed." This suggests that a search occurs well before the government reviews the data, and likely at the moment the electronic communication service produces the information. That production, like the execution of the warrant, should be considered to have taken place where the communications service is located.

D. The Government's Mischaracterizations of the Record

Regrettably, DreamHost again finds it necessary to address the government's mischaracterizations of the record. To begin with, DreamHost reiterates that the parties are before the Court not because of any failure by DreamHost, but because of the government's failure to respond to or address the concerns expressed in a timely manner by DreamHost about the government's subpoena and the Search Warrant, which the government now concedes was, and still remains, an ill-informed attempt to gather a large amount of information concerning third-parties.

[5] The Search Warrant was personally served on DreamHost in California by an FBI Agent. See July 18, 2017 E-mail from AUSA Borchert to DreamHost employee Karl Fry ("You were personally served by the FBI yesterday.") The government does not and cannot explain how such facts constitute "execution" in Washington, D.C.

The government claims that it "attempted to have a dialogue with DreamHost about these matters," and that "those attempts have proven unproductive because DreamHost maintains that the Warrant is improper and that the court lacks jurisdiction to issue the warrant." (Reply at 4.) To the contrary, it was DreamHost, and not the government, who attempted to clarify the scope of *both* the subpoena and the search warrant. Instead of engaging in a conversation with DreamHost, AUSA Borchert ignored DreamHost's requests, (1) in the case of the subpoena, threatening to obtain a court order instead of answering DreamHost's inquiries, and (2) in the case of the search warrant, completely ignoring DreamHost's e-mail seeking clarification and, instead, filing its now infamous motion to compel. (Opp'n at 5-6.) The government acts in bad faith when it characterizes DreamHost's actions in a negative light, seeking only to justify its unprofessional conduct.

The government also fails to acknowledge its improper requests for additional information in violation of the Stored Communications Act. In his email to DreamHost's outside counsel, AUSA Borchert asked "How many visits were there to the website prior to January 21, 2017?" Counsel properly responded by telling AUSA Borchert that DreamHost "cannot readily give the government such information without a proper request." (Reply Ex. 1.) Yet, the government flaunts its clear and brazen attempts to bypass and violate the law and the obligations imposed upon it under the Stored Communications Act in seeking such information.

Further, the government argues that this exchange, along with DreamHost's request that the government properly serve its subpoena and warrant, is an example of DreamHost's

"months-long attempt to avoid compliance with lawful court orders."[6] DreamHost stands by every aspect of its requests for proper legal process and clarification concerning the Search Warrant. While the government may have become accustomed, and may in fact expect, that it not be questioned or inconvenienced by a third party, DreamHost has an obligation not only to its users pursuant to company policy, but also more broadly via the Electronic Communications Privacy Act, the Privacy Protection Act and various other governing laws. Had the government entertained DreamHost's requests to discuss the scope of the warrant instead of filing its motion to compel, these issues may have been avoided altogether. But, alas, it was the government's decision to ignore DreamHost's inquiries and escalate the issues presented by the Search Warrant.

The government claims that some of the information DreamHost brought to light was "unknown to the government and the Court at the time the Warrant was issued." (Reply at 14.) However, counsel for DreamHost clearly outlined the exact issues in an email to AUSA Borchert on Friday, July 21 (Raymond Aghaian's Email on Friday, July 21 to AUSA Borchert explaining issues with warrant). From that point, the government was explicitly, and in no unclear terms, on notice that the warrant would force DreamHost to produce data that included, among other things, the IP addresses and data protected by the Privacy Protection Act.[7] The government's argument that these additional facts "were unknown" is

[6] In one instance, AUSA Borchert issued a subpoena to DreamHost on February 8, 2017 asking for production of records on February 6, 2017, two days prior to service of the subpoena. The government interprets DreamHost's request for issuance of a new subpoena with the accurate response date as an example of non-compliance.

[7] The government's filing strategy further underscores its gamesmanship. Having made no previous effort to seal any materials in this proceeding, on Monday, August 21, 2017, the government sought to seal its Reply, contending that the filing contained secrecy issues under Rule 6(e), although it noted that it "does not oppose the Court exercising its discretion under Rule 6(e)(3)(E)(i) and issuing an order that authorizes that any filings and any hearings on this matter be made public." Before the Court could rule on the government's sealing request, however, the government publically filed the Reply late Tuesday afternoon, August 22, 2017, timing its filing mainly to minimize additional media coverage.

entirely misleading. Only now, after worldwide press coverage, does the government allege that it "has no interest in records relating to the 1.3 million IP addresses." (Reply at 3-4.) Yet, incredibly, it maintains the frivolous contention that the original warrant was "lawful and appropriate."

The record before the Court reflects the disingenuous conduct by the government. While DreamHost is not seeking sanctions, the government's bad faith conduct, and its frivolous litigation positions can be deemed as sanctionable conduct under the Hyde Amendment. United States v. Wade, 255 F.3d 833, 836 (D.C. Cir. 2001) ("[T]he court, in any criminal case…may award to a prevailing party…a reasonable attorney's fee and other litigation expenses, where the court finds that the position of the United States was vexatious, frivolous, or in bad faith.") (citing Hyde Amendment, Pub. L. No. 105-119, 111 Stat. 2440, 2519 (1997)); United States v. Pocklington, 831 F.3d 1186, 1188 (9th Cir. 2016) ("We have described a frivolous position as 'groundless…with little prospect of success; often brought to embarrass or annoy the defendant.'") (quoting United States v. Braunstein, 281 F.3d 982, 995 (9th Cir. 2002)).

///

///

III. Conclusion

For the foregoing reasons, DreamHost respectfully requests that the government's motion to compel as well as its motion to modify Attachment B of the Search Warrant be denied.

Dated this 23re day of August, 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 to be 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

I hereby certify that true and correct copy of the foregoing was sent via e-mail this 23rd day of August, 2017, to:

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

Paul Alan Levy
Public Citizen Litigation Group
1600 20th Street, NW
Washington, D.C. 20009
plevy@citizen.org

/s/ Raymond O. Aghaian
Raymond O. Aghaian

ATTACHMENT B

Particular Things to be Seized

I. **Information to be ~~disclosed~~Disclosed by DreamHost**

To the extent that the information described in Attachment A ("the Account") is within the possession, custody, or control of DreamHost, 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), DreamHost is required to disclose the following information to the government for ~~each account or identifier listed in Attachment A~~the Account:

a. **for the time period from July 1, 2016, through and including all of January 20, 2017 (Eastern Time),** all records or other information, pertaining to ~~that account or identifier~~the Account, including all files, databases, and database records stored by DreamHost in relation to that ~~account or identifier;~~Account; AND

b. all information in the possession of DreamHost that might identify the DreamHost subscribers related to ~~those accounts or identifiers~~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; AND

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

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 the content of any unpublished draft publications (e.g., draft blog posts), including images (and metadata for those images) that were associated with draft publications.

f. DreamHost shall not disclose records that constitute IITTP request and error logs.

II. Information to be ~~seized~~Seized by the Government

A. Description of the Evidence

The government~~All~~ may seize all information described above in Section I that constitutes ~~fruits,~~ evidence ~~and instrumentalities~~ of the violations of D.C. Code ~~§ 22-1322 involving the~~§§ 22-1322, 22-1805a, and 22-303, that are described in the Affidavit attached to this Warrant and that are **(or** have been) the subject of the criminal prosecutions (described in paragraph 11 of the Affidavit), including:

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

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

(c) evidence, including Internet Protocol **("IP")** addresses, e-mail addresses, and any other evidence that will help identify individuals who participated~~,~~

~~planed, organized, or incited the January 20 riot,~~ in the above-described offenses, planned for the above-described offenses, organized the above-described offenses, or incited the above-described offenses; and

(d) evidence about the state of mind of individuals who participated (or, knowing about planned violence, refused to participate) in the above-described offenses, planned for the above-described offenses, organized the above-described offenses, or incited the above-described offenses.

B. Types of Information Within the Scope of Part (II)(A)

For evidence that is within the scope of Part II(A) of this Attachment B, the government may seize all information relating to the development, publishing, advertisement, access, use, administration or maintenance of any website enumerated in Attachment A, including:

1. ~~Files~~files, databases, and database records stored by DreamHost on behalf of the subscriber or user operating the ~~website~~Account, including:

a~~. programming code used to serve or process requests made via web browsers;~~b. HTML, CSS, JavaScript, image files, or other files; ~~HTTP request and error logs;~~

~~c~~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;

~~d~~c. MySQL, PostgreSQL, or other databases related to the website;

~~e. email accounts and the~~d. The contents ~~thereof, associated with the account;~~of e-mail accounts that are within the @disruptj20.org domain (including info@disruptj20.org).

2. ~~Subscriber~~DreamHost subscriber information ~~related to the accounts established to host the site enumerated in Attachment A~~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. ~~If a domain name was registered on behalf of the subscriber, the~~The date that the domain name disruptj20.org was registered~~, the domain name~~, 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.

~~DreamHost shall deliver the information set forth above via United States mail, courier, or email to the following:~~

~~John W. Borchert~~

~~Assistant U.S. Attorney~~

~~U.S. Attorney's Office for the District of Columbia~~

~~555 Fourth Street, N.W.~~

~~Washington, D.C. 20530~~

~~Email: John.BorchertOusdoj.gov~~

~~Telephone: 202-252-7679~~

Subject to the procedures discussed in Part III of this Attachment B, the government is authorized to retain a digital copy of all information disclosed by DreamHost, for as long as it is necessary for purposes of authentication at trial.

III. Procedures for Handling Information Disclosed by DreamHost

The government will conduct a search of the information produced by DreamHost and determine which information is within the scope of the information to be seized specified in Section II. That information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from DreamHost that does not fall within the scope of Section II and will not further review the information absent an order of the Court.