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

IN THE MATTER OF THE SEARCH OF WWW.DISRUPTJ20.ORG THAT IS STORED AT PREMISES OWNED, MAINTAINED, CONTROLLED, OR OPERTED BY DREAMHOST	Special Proceedings No. 17 CSW 3438

GOVERNMENT'S REPLY IN SUPPORT OF ITS MOTION TO SHOW CAUSE, AND MOTION TO MODIFY ATTACHMENT B OF THE SEARCH WARRANT

The United States, by and through its attorney, the United States Attorney for the District of Columbia, respectfully submits this reply brief in support its motion to show cause and respectfully moves this Court modify Attachment B of the search warrant in light of factual revelations since July, 2017. In support of its position, the United States relies on the following points and authorities, and such other points and authorities as may be cited at a hearing on the motions.

BACKGROUND

On July 12, 2017, a Judge of this Court issued a valid search warrant (hereinafter, the "Warrant") that directed DreamHost Inc. ("DreamHost") to provide specific, particularized categories of information associated with the website disruptj20.org. The affidavit submitted in support of the search warrant (the "Affidavit") demonstrated that the website disruptj20.org was used to organize a riot that took place in the District of Columbia on the morning of January 20, 2017. The rioters – some of them armed with hammers, crow bars, wooden sticks and other weapons – moved as a cohesive unit for approximately thirty (30) minutes, traveling more than a dozen city blocks, as individual participants engaged in violence and destruction that caused hundreds of thousands of dollars' worth of property damage and left civilians and officers injured.

The government values and respects the First Amendment right of all Americans to participate in peaceful political protests and to read protected political expression online. This Warrant has nothing to do with that right. The Warrant is focused on evidence of the planning, coordination and participation in a criminal act – that is, a premeditated riot. The First Amendment does not protect violent, criminal conduct such as this.

When the Warrant was issued, it was supported by probable cause and it met all other legal and constitutional requirements. The Warrant – like the government's investigation into the criminal conduct that occurred on January 20, 2017 in the District of Columbia – was specifically directed at evidence of a crime (violations of D.C. Code § 22-1322) "involving the individuals who participated, planned, or incited the January 20 riot." The Warrant is part of the on-going criminal investigation that has resulted in nineteen guilty pleas and almost two hundred other pending criminal cases against individuals charged (by an indictment issued by a Grand Jury) for their role and participation in the January 20th riot. The Affidavit establishes probable cause to believe that, before January 20, 2017, disruptj20.org was used by a small and focused group of individuals. The Website was not just a means to publicly disseminate information (as many websites are designed to do), but was also used to coordinate and to privately communicate among a focused group of people whose intent included planned violence. For example, as shown in the Affidavit, the site was even used to verify the identity of people in closely-held meetings that were not open to the media or public, where organizers required attendees to log-in to the website to prove their credentials. The website does not appear to have been updated since the first week of February 2017, and the vast majority of information on the website appears to pre-date January 20, 2017.

The Warrant—like the criminal investigation—is singularly focused on criminal activity. It will not be used for any other purpose. Contrary to DreamHost's claims, the Warrant was not intended to be used, and will not be used, to "identify the political dissidents of the current administration[.]" (Opp. at 1.)[1] Nor will it be used to "chill[ ] free association and the right of free speech afforded by the Constitution."[2] In fact, as discussed further below, after conducting a careful search and seizing the evidence within the scope of the Warrant, law enforcement will set aside any information that was produced by DreamHost but is outside the scope of the Warrant; it will seal that information; and it will not revisit that information without a further court order.

The government is acutely aware that criminal investigations involving electronic evidence present unique challenges. One of those challenges is that some of the evidence – particularly the full scope of the evidence – will be hidden from the government's view unless and until the government obtains a court order or search warrant. That is an important part of the history in this case because much of DreamHost's challenge to the Warrant is based on information that was not known (and would not reasonably have been known) to the government when the Warrant was applied for and obtained. What the government did not know when it obtained the Warrant – what it could not have reasonably known – was the extent of visitor data maintained by DreamHost that extends beyond the government's singular focus in this case of investigating the planning, organization, and participation in the January 20, 2017 riot. The government has no interest in

---

[1] It is disingenuous for DreamHost to characterize the individuals behind "DisruptJ20" merely as opponents of the current President of the United States. The DisruptJ20 organizers have publicly stated that they "would be dissatisfied with any U.S. leader," that they began planning the DisruptJ20 events when "Hillary Clinton was the clear front-runner," and they "protested President Barack Obama's second inauguration, too." Perry Stein, *What Draws Americans to Anarchy? It's more than just smashing windows,* Washington Post, August 10, 2017, available at https://www.washingtonpost.com/local/public-safety/ (last visited Aug. 15, 2017).

[2] *See* DreamHost, *We Fight for the Users*, DreamHost.blog (last visited August 15, 2017).

records relating to the 1.3 million IP addresses that are mentioned in DreamHost's numerous press releases and Opposition brief. The government's investigation is focused on the violence discussed in the Affidavit. Consistent with that focus, the government is asking this Court to enter a new Attachment B to the Warrant, and remains committed to minimizing the information that is ultimately seized for the government's criminal investigation.

Notably, the government has attempted to have a dialogue with DreamHost about these matters. Regrettably, those attempts have proven unproductive because DreamHost maintains that the Warrant is improper and that the Court lacks jurisdiction to issue the Warrant. (Mot. at Ex. G.) As recently as this past week, DreamHost told the government that it would provide no information about the Website without further legal process and—somewhat incompatibly—told the government that DreamHost would only discuss limiting the production of information called for by the Warrant if the government first withdrew the Warrant in its entirety. (Ex. 1.)[3]

The government requests that the Court take two steps to resolve this matter. First, the Court should reject DreamHost's legal arguments that question the Court's legal authority to issue the Warrant and challenge the lawfulness of the two-step process being used in this case. Second, the government requests that the Court amend the Warrant with the new proposed Attachment B. Based on new information presented by DreamHost in response to the Motion to Show Cause (and

[3] These recent communications from DreamHost are simply the latest example in a months-long attempt to avoid compliance with lawful Court orders. DreamHost refused to honor a grand jury subpoena unless it was served upon them personally; then, once a copy of the subpoena was hand-served (on February 8, 2017), DreamHost informed the government that they were working on compliance. Weeks later (and after multiple inquiries by the government and promises by DreamHost that this was in the "queue" and that they were working on production), DreamHost refused to comply with the subpoena because the return date had passed. (Ex. 2). Personal service was effected a second time with a new subpoena calling for precisely the same records as the first subpoena. More recently, the general counsel of the company promised to provide "production information and instructions" to the government in response to the Warrant by July 20, 2017, but then one day later told the government—through outside counsel—that the Warrant was invalid.

in DreamHost's press release), the government has refined and modified Attachment B. The government submits that this modified Attachment B renders moot the remaining arguments advanced by DreamHost.[4] With the modified Attachment B, the valid and lawful Warrant (for which probable cause was found and still plainly exists) should be enforced.

ARGUMENT

I. The Search Warrant is Neither Extraterritorial Nor Unlawful

DreamHost challenges this Court's jurisdiction to issue any search warrant under the Stored Communications Act ("SCA") 27 U.S.C. § 2701, *et seq*, claiming that the Warrant is an unlawful extraterritorial search warrant under the D.C. Code. In advancing this argument, DreamHost demonstrates that it has a fundamental misunderstanding of search warrants under the SCA, the D.C. Code, and the D.C. Superior Court Rules of Criminal Procedure.

A. Under the SCA, this Court has the Authority to Issue Search Warrants Directed at U.S. Providers of Electronic Communication Services and Remote Computer Services, Regardless of the Providers' Location

As recently explained by Chief Judge Howell in *In re Search of Information Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google Inc.* ("*Google*"), 2017 WL 344634 (D.D.C. July 31, 2017), the "SCA regulates how stored wire and electronic communications may be lawfully accessed or disclosed. Among other things, the SCA's § 2703, permits the government, in specified circumstances, to compel service providers to disclose records or information pertaining to their customers as well as the contents of their customers' stored electronic communications." An SCA search warrant is a "distinct procedural mechanism

[4] As noted in Section III, *infra*, the Warrant (with the original Attachment B) is valid and enforceable. In crafting the modified Attachment B, the government has done what it tried to do informally (and unsuccessfully) with DreamHost – that is, focus on potential evidence of the criminal offenses under investigation based on all the information now known to the government.

from a traditional Rule 41 search warrant," *id.*, and, "in particular, by 2001, Congress ensured that an SCA warrant was not bound by Rule 41(b)'s venue restrictions" by clarifying that federal magistrate judges were authorized to issue SCA warrants to providers located in other judicial districts, and by authorizing state courts to issue SCA warrants to U.S. providers without any geographic restriction.

Specifically, Section 2703 of the SCA permits any "court of competent jurisdiction" to issue SCA legal process, and Section 2711 defines "court of competent jurisdiction" to include:

> (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—
>
> (i) has jurisdiction over the offense being investigated;
>
> (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or
>
> (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title; or
>
> (B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants[.]

18 U.S.C. § 2711(3). The term "State," as used in the SCA, includes the District of Columbia. *See* 18 U.S.C. § 2711(1) *with* 18 U.S.C. § 2510(3).

The SCA does impose some limitations on SCA warrants issued by federal district courts. Primarily, federal courts must either have "jurisdiction over the offense being investigated," or be "in … a district in which the provider is located." 18 U.S.C. § 2711(3)(A). However, as DreamHost acknowledges (at 18 n.7), the SCA imposes no such limits on State courts. Thus, the SCA empowers any State "court of general criminal jurisdiction" that is "authorized by law … to issue search warrants" to issue SCA warrants, without any additional geographic requirement.

That federal grant of authority was sufficient to authorize this Court to issue SCA warrants, even without any further action by the District of Columbia. While D.C. Code § 23-521(a) states that the Court "may" issue warrants that "authorize a search to be conducted anywhere in the

District of Columbia," it does not in any way purport to limit the Court's powers under the SCA. Similarly, while D.C. Superior Court Rule of Criminal Procedure 41(f)(2) states that D.C. Code search warrants "may be executed anywhere within the District of Columbia," that rule does not purport to modify the scope of the SCA – and DreamHost has not identified any authority that supports its claim to the contrary. DreamHost has not cited any case concluding that any State court of general jurisdiction lacks authority to issue SCA search warrants. In fact, in its brief discussion of the issue (at 17-18), DreamHost relies entirely on cases that reach the opposite result. *See In re Search Warrant for Records from AT&T*, 2017 WL 2511269 at *4, -- A.3d -- (N.H. 2017) (upholding circuit court's authority to issue search warrant to AT&T in Florida); *Oregon v. Rose*, 330 P.3d 680, 686 (Ore. 2014) (finding that Oregon law "authorizes an Oregon court to issue a search warrant to be executed on a business outside of Oregon so long as the court has personal jurisdiction over the recipient business"); *Hubbard v. Myspace, Inc.*, 788 F. Supp. 2d 319 (SCA search warrant was valid, even though it exceeded the "ordinary territorial authority" of the issuing state court). DreamHost's jurisdictional challenge should be rejected on that basis alone.

B. In This Case, Neither The Execution Nor the Search Are Extraterritorial

Finally, nothing in D.C. Code § 23-521(a) and Rule 41(f)(2) suggests the Court lacks authority to issue the Warrant, as both the execution and the search authorized by the Warrant in this case are actions within the District of Columbia, and none of the relevant conduct is "extraterritorial." The Warrant was issued in the District of Columbia, it was executed in the District of Columbia, it was served on a provider with contacts in the District of Columbia, and the search will be conducted in the District of Columbia. DreamHost's contrary conclusion depends on a fundamental misunderstanding of SCA search warrant law and procedure.

The procedure for implementing SCA search warrants differs from the procedure for traditional premises and property search warrants, which typically must be executed by law enforcement officers, and which commonly authorize law enforcement officers to enter private property without the consent of the owner or occupant. In contrast, SCA search warrants are executed by simply serving the search warrant upon the designated provider, an act which is typically accomplished by e-mail, fax, or other electronic delivery. This manner of execution does not require law enforcement officers physically to enter upon the property of the provider; it can be accomplished remotely. Indeed, the Warrant in this case specifically authorized the Metropolitan Police Department to "execute" the Warrant "by emailing or faxing" the provider.

An SCA warrant so executed then requires the designated provider to disclose information to law enforcement, and then authorizes law enforcement to search that information for evidence. The "search" thus occurs when—and where—law enforcement reviews the information provided. This process was recently explained by Chief Judge Howell in the *Google* decision. As the court explained,

> [I]n the context of electronic information, when Google queries its database, finds the communications in question, and retrieves it for storage on its local servers in the United States, Google does not "search" or "seize" the communications in a Fourth Amendment sense. The Fourth Amendment protects two types of expectations, one involving 'searches' the other 'seizures.'. . ._A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. . . . A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."

2017 WL 3445634 at * 16 (citations omitted). The court further explained that a provider's internal handling of subscriber information – wherever that occurs – "does not amount to a "search" or a "seizure" in any meaningful sense, because such providers routinely control that information without infringing on "any expectation of privacy" or "meaningfully interfere[ing] with the

customer's possessory interests." *Id.* Critical to that decision, the impingement on subscriber privacy – that is, the constitutional "search" and "seizure" that is the subject of a search warrant – occurs in the location where law enforcement reviews that subscriber's information. Thus, in this case, the search will occur within the District of Columbia, when the Metropolitan Police Department reviews the information disclosed by DreamHost.

While D.C. Code § 23-521(a) states that the Court "may" issue warrants that "authorize a search to be conducted anywhere in the District of Columbia, it does not in any way purport to limit the Court's powers under the SCA, and in any event, the SCA search at issue will, in fact, "be conducted … in the District of Columbia." Similarly, while the D.C. Superior Court Rule of Criminal Procedure 41(f)(2) specifies that D.C. Code search warrants "may be executed anywhere within the District of Columbia," that rule does not purport to modify the scope of the SCA, and in any event, the execution specified in the Warrant actually took place in the District of Columbia.

II. The Warrant's Two-Step Disclose-and-Search Process Is Reasonable, Appropriate, and Entirely Lawful.

The two-step procedure incorporated into the Warrant is a practical necessity for search warrants directed at electronically stored information. It has been approved by courts around the country, including every federal appellate court that has examined the issue. *See United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012) ("[t]he federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a 'sufficient chance of finding some needles in the computer haystack.'"); *United States v. Stabile*, 633 F.3d 219, 233-34 (3d Cir. 2011) ("practical realities of computer investigations preclude on-site searches"); *United States v. Grimmett*, 439 F.3d 1263, 1268–70 (10th Cir. 2006) (search warrant for "any and all" computer

hardware and software for child pornography authorized both the seizure and subsequent search of the defendant's computer files); *Guest v. Leis*, 255 F.3d 325, 335 (6th Cir. 2001) ("Because of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers, including their content, was reasonable in these cases to allow police to locate the offending files."); *United States v. Hay*, 231 F.3d 630, 637-38 (9th Cir. 2000) (off-site search was appropriate "because of the time, expertise, and controlled environment required for a proper analysis"); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) ("the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images [of the child pornography sought].").

The two-step procedure is appropriate for electronic device search warrants, but it is particularly applicable to search warrants issued under the SCA. *See, e.g., United States v. Bach*, 310 F.3d 1063, 1065 (8th Cir. 2002) (upholding as consistent with the Fourth Amendment a procedure in which "Yahoo! technicians retrieved all of the information from Bach's account" and then did "not selectively choose or review the contents of the named account."); *United States v. Patel*, No. 16-CR-798 (KBF), 2017 WL 3394607, at *4 (S.D.N.Y. Aug. 8, 2017) ("the above principles make clear that executing authorities may obtain the entire contents of an email account in an effort to search for a more limited set of emails"); *In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc.*, 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014), as amended (Aug. 7, 2014) ("Notably, every case of which we are aware that has entertained a suppression motion relating to the search of an email account has upheld the Government's ability to obtain the entire contents of the email account to determine which particular emails come within the search warrant."). The district court's decision in *In the Matter of the Search of Information Associated with*

[redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F.Supp.3d 157 ("*Apple II*") (D.D.C. 2014), is instructive. The search warrant in that case required Apple to produce information without first screening it for evidentiary value, and it authorized the government to search that information. The court found that this procedure was both reasonable and consistent with the requirements of the Fourth Amendment. The court also explained the "nettlesome problems" of permitting providers to filter data before disclosing it to the government:

> [I]t would be unworkable and impractical to order Apple to cull the e-mails and related records in order to find evidence that is relevant to the government's investigation. To begin with, non-governmental employees untrained in the details of the criminal investigation likely lack the requisite skills and expertise to determine whether a document is relevant to the criminal investigation. Moreover, requiring the government to train the electronic service provider's employees on the process for identifying information that is responsive to the search warrant may prove time-consuming, increase the costs of the investigation, and expose the government to potential security breaches.

Id. at 166-167. Finally, the court emphasized the Supreme Court's instruction that, although the search would always be subject to subsequent judicial review, a "search warrant's execution is 'generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant[.]'" *Id.* (citing *Dalia v. United States*, 441 U.S. 238, 257 (1979)).

DreamHost ignores the emerging consensus on these points. DreamHost fails to cite any case showing that evidence was suppressed based on the application of the two-step procedure, and instead focuses on cases showing that a few magistrate judges have denied search warrant applications that employ the procedure. The cases DreamHost cites are obvious outliers – and they either involve factors not present in this case, or they have been vacated or superseded by subsequent case law. For example, *In the Matter of the Search of Information Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 25 F.Supp.3d 1 ("*Apple*

I") (D.D.C. 2014), was vacated by the decision in *Apple II*. Similarly, *In re Search of Premises Known as Three Hotmail Email Accounts*, 2016 WL 1239916 (D. Kan. 2016), was overruled in relevant part by *In re Search of Information Associated With Email Addresses Stored At Premises Controlled By Microsoft*, 212 F. Supp. 3d 1023 ("*Microsoft*") (D. Kan. 2016) – and in *Microsoft*, the district court expressly held that the two-step procedure for the search of e-mail accounts complied with the Fourth Amendment. *Id.* at 1030. DreamHost likewise fails to mention that *In re: [Redacted]@gmail.com*, 62 F. Supp. 3d 1100 (N.D. Cal. 2014) , involved strikingly different circumstances, addressing (1) a warrant which had already been denied in the District of Columbia "for the reasons stated in" *Apple I*, which has since been overruled; and (2) which was then re-presented, without modification, in the Northern District of California; and (3) the government had made no commitment to set aside items that were outside the scope of the warrant. *Id.* at 1104. The government in this case has not engaged in any similar conduct – and, as noted above, the government is committed to sealing and setting aside any information that is not within the scope of Part II of Attachment B and has proposed significant refinements to Attachment B as discussed below.

Finally, and more fundamentally, DreamHost has not provided any basis to believe that the two-step procedure is unreasonable in this case – and it has not provided any basis to believe that an alternative procedure is even practical. There is no evidence that DreamHost personnel can adequately search DreamHost records to determine "whether a [particular] document is relevant to the criminal investigation." *Apple II* at 166-167. DreamHost simply asserts, without more, that the two-step procedure is "not without controversy." Opposition at 11. That is not the standard. For all of the foregoing reasons, the two-step procedure is appropriate, reasonable, and lawful

under the Fourth Amendment – and it is the only workable method of identifying the evidence that is the subject of the Warrant.

III. The Court Should Enforce the Warrant with the Government's Proposed Modified Attachment B.

A. The Warrant

The Judge who issued the Warrant in July 2017 correctly found probable cause to believe that evidence relevant to the government's criminal investigation into the riot that occurred on January 20, 2017, would be found within the "Information to be Disclosed" that is described in Part I of Attachment B of the Warrant. The resulting Warrant (1) required DreamHost to disclose the "Information to be Disclosed" to law enforcement, and (2) authorized law enforcement to search the information disclosed by DreamHost and to seize the "Information to be Seized" that is described in Part II of Attachment B. The "Information to be Seized" described in the original Attachment B must meet three specific criteria. It must: (1) constitute fruits, evidence and instrumentalities of violations of D.C. Code 22-1322 (rioting statute); (2) involve the individuals who participated, planned, organized or incited the January 20 riot; and (3) relate to the development, publishing, advertisement, access, use, administration or maintenance of disruptj20.org. The Warrant identifies the specific property to be searched by describing the particular account information that DreamHost must disclose (in Attachment A and Part I of Attachment B), and it then specifies the particular information to be seized (in Part II of Attachment B), *i.e.*, records and files that constitute fruits, evidence or instrumentalities of a specific criminal offense (22 D.C. Code, Section 1322) that was committed on a specific date (January 20, 2017).

B. The Government Requests that Attachment B of the Warrant Be Modified in Light of DreamHost's Recent Disclosures.

As noted above, the Warrant was properly issued by the Court and contains appropriate and recognized procedures. Over the past week, DreamHost has made numerous public statements and made many statements in its opposition brief which provide information about the website that were unknown to the government and the Court at the time that the Warrant was issued. Both the government and the Court are now aware of the following:

- "During the time period January 23, 2017 to January 28, 2017, DreamHost has maintained HTTP logs for over 1,300,000 IP addresses of visitors to the website" which is a time period after the riot at issue in the government's case. (Fry Decl. ¶ 5.)
- "DreamHost maintains emails associated with the Website, including emails of third parties." (Fry Decl. ¶ 6.) "The Website proposes several email addresses within the disruptj20.org domain name and invites correspondence." (Opp. at 8.)
- "DreamHost maintains membership lists for several email discussion lists, from a number of different email accounts sponsored by the website." (Fry Decl. ¶ 7.)
- "DreamHost maintains over 2,000 images related to the Website. (Fry Decl. ¶ 8.)
- DreamHost maintains some "unpublished" materials such as "draft blog posts" and "hundreds of images." (Fry Decl. ¶¶ 10, 11.)

To re-iterate: these additional facts were unknown to the government at the time it applied for and obtained the Warrant; consequently, the government could not exclude from the scope of the Warrant what it did not know existed. The Affidavit, the indictment that was returned by a Grand Jury, and the government's repeated statements made during public hearings in the pending criminal cases make clear that the government is focused on the criminal acts of defendants and

their co-conspirators, and not their political views – and certainly not the lawful activities of peaceful protesters. Similarly, the government is focused on the use of the Website to organize, to plan, and to effect a criminal act – that is, a riot. The government has no interest in seizing data from the Website that does not relate to this limited purpose. Committed to the limited purpose of investigating the criminal conduct involved in the organization, planning, and execution of a riot on January 20, 2017, the government has taken the new information provided by DreamHost and modified Attachment B to carve out data and information that the government does not seek.[5]

---

[5] Although, based on the new information provided by DreamHost, the government seeks to refine Attachment B, the original Attachment B was nonetheless lawful and appropriate. The original Attachment B specifically identified the property to be searched by describing (in Attachment A and Part I of Attachment B) the particular account information that DreamHost must disclose, and it then specifies (in Part II of Attachment B) the particular information to be seized: records and files that constitute fruits, evidence or instrumentalities of a specific criminal offense that was committed on a specific date. These specifications, together with description of the offenses in the Affidavit (which is attached to the Warrant), satisfy the Fourth Amendment. *Compare Microsoft*, 212 F. Supp. 3d 1023, 1026-1027 (upholding search warrant that sought all information associated with particular Microsoft accounts, without any date limitation for the information to be disclosed; identified relevant criminal statutes and the dates of the violations; and then authorized the recovery of, among other things, "Evidence indicating the email account owner's state of mind as it relates to the crime under investigation.").

Moreover, in addition to the three limitations in Part II of Attachment B, the original Warrant described specific types of files that the government seeks to seize, and the Affidavit provided additional context and clarity for the scope of the Warrant as a whole, including the limitations in Part II of Attachment B. The Affidavit, attached to the Warrant, demonstrated that the original Warrant concerns information related to the specific crimes that led up to, and constituted, the January 20, 2017 riot. *See United States v. Moore*, 263 A.2d 652 (D.C. 1970) (finding that warrant described the place to be searched with sufficient particularity, where "the affidavit was attached to the warrant and sufficiently referred to therein to enable the officers executing the warrant to look at the affidavit and determine the place intended"). *Cf. Apple II*, 13 F. Supp. 3d at 164 (noting that the affidavit included "additional background information on the particular types of records that must be disclosed, the specific crimes for which the government seeks evidence, and the targeted entities and individuals," and emphasizing that, "when read together with the affidavit, the government's application provides detailed information of the alleged criminal scheme and a thorough explanation for why evidence relevant to the investigation is likely to be found in e-mail records and other data related to the target email account").

Part I of the modified Attachment B (the information to be disclosed by DreamHost) has been refined in the following ways: (1) DreamHost should only provide content and transactional information for the time period from July 1, 2016, through and including January 20, 2017, which covers the time frame described in the Warrant, Affidavit, the date when the site was purchased, and the public statements made by organizers of DisruptJ20 regarding the timing of the organization and planning (Ex. 3 at I.a.); (2) DreamHost should not disclose the contents of unpublished draft publications, including images and their metadata (Ex. 3 at I.e.); and (3) DreamHost should not disclose records that constitute HTTP request and error logs (Ex. 3 at I.f.).

Part II of the modified Attachment B (the information to be seized by the government) also provides more detailed descriptions regarding the types of information that will be seized by the government.

Part III of the modified Attachment B (procedures for handling information disclosed by DreamHost) also sets forth what will happen to the evidence that is not seized by the government during its search of the materials provided by DreamHost – that is, the government will have such information placed under seal with the Court and will not copy or retain such information for any further purpose. (Ex. 3 hereto at II.B.)

The government believes that, collectively, these modifications to Attachment B minimize the disclosure of data that is not directly related to the criminal investigation, thereby reducing the burden on DreamHost to disclose information and reducing the burden on the government to conduct its search. Such modifications should amply address the First Amendment/Fourth Amendment reasonableness concerns raised by DreamHost. Similarly, the government's modifications are designed to clarify that the government is not seeking access to

any "work product" that is potentially covered by the Privacy Protection Act, as that term is defined in 42 U.S.C. § 2000aa-7(b).

CONCLUSION

For the foregoing reasons and any other reasons that may be cited at a hearing on this motion, the government requests that the Court amend the Warrant with the government's proposed modified Attachment B, and grant the government's request that DreamHost be compelled to comply with the Warrant.

Respectfully submitted,

CHANNING D. PHILLIPS
UNITED STATES ATTORNEY

By: /s/ Jennifer A. Kerkhoff

Jennifer A. Kerkhoff
John W. Borchert
Assistant United States Attorneys
United States Attorney's Office for the
District of Columbia
555 Fourth Street, N.W.
Washington, D.C. 20530

August 21, 2017

CERTIFICATE OF SERVICE

I hereby certify that copy of the foregoing was delivered via electronic mail to counsel for DreamHost this 21st day of August 2017.

/s/ Jennifer A. Kerkhoff
Jennifer A. Kerkhoff
Assistant United States Attorney

EXHIBIT 1

From: Aghaian, Raymond
To: Borchert, John (USADC)
Cc: Kerkhoff, Jennifer (USADC)
Subject: RE: DreamHost matter
Date: Thursday, August 17, 2017 1:37:56 PM

Hi John,

Your question below about the website is seeking information that is governed by the Stored Communications Act. We cannot readily give the government such information without a proper request.

Moreover, we were trying to discuss the issue of narrowing the scope of your search warrant to provide you with records as expeditiously as possible before you went silent and filed the motion to compel. Happy to have such a discussion, once the motion and search warrant are withdrawn.

Ray

Raymond O. Aghaian
Kilpatrick Townsend & Stockton LLP
9720 Wilshire Blvd PH | Beverly Hills, CA 90212-2018
office 310 310 7010 | fax 310 388 1198
raghaian@kilpatricktownsend.com | My Profile | vCard

From: Borchert, John (USADC) [mailto:John.Borchert@usdoj.gov]
Sent: Wednesday, August 16, 2017 10:07 AM
To: Aghaian, Raymond
Cc: Kerkhoff, Jennifer (USADC)
Subject: DreamHost matter

Hello, Ray –

We noticed in your opposition that "[d]uring the time period January 23, 2017 to January 28, 2017, DreamHost has maintained HTTP logs for over 1,300,000 IP addresses of visitors to the website." How many visits were there to the website prior to January 21, 2017? That information might be helpful in narrowing the issues for the court to consider.

Also, assuming that the Court determines that its search warrant is valid, are there any materials called for by the warrant that DreamHost does not object to producing to the government?

Regards,

John

John W. Borchert
Deputy Chief -- Felony Major Crimes Trial Section
Misdemeanor Trial Unit
U.S. Attorney's Office for the

District of Columbia
Desk: 202-252-7679 Mobile: 202-870-6071
john.borchert@usdoj.gov

EXHIBIT 2

From: Karl Fry
To: Borchert, John (USADC); legal@dreamhost.com
Cc: O"Rourke, Allen (USADC); Kerkhoff, Jennifer (USADC); christopher.ghazarian@dreamhost.com
Subject: Re: Dreamhost - Preservation Request (LGL-53782)
Date: Wednesday, February 22, 2017 7:53:59 PM

Hi John,

Thank you for your ongoing patience.

We're still processing our queue and haven't been able to address this subpoena yet. In reviewing the subpoena we've noticed that the production date is February 6th, while the subpoena itself was served on February 8th (after the date of production). We kindly ask that you issue another subpoena with a proper deadline (2 weeks is acceptable). We will accept service by email this time.

Thank you,
Karl Fry
DreamHost Compliance Team
http://www.dreamhost.com

On 2/22/17 1:59 PM, Borchert, John (USADC) wrote:

> Hello, Karl - I thought I should circle back. Can you update us?
>
> Regards,
>
> John
>
> John W. Borchert
> Assistant United States Attorney
> U.S. Attorney's Office for the
> District of Columbia
> Desk: 202-252-7679 Mobile: 202-870-6071
> john.borchert2@usdoj.gov
>
> **From:** Karl Fry [mailto:karl.fry@dreamhost.com]
> **Sent:** Thursday, February 16, 2017 2:31 PM
> **To:** Borchert, John (USADC) <JBorchert@usa.doj.gov>; legal@dreamhost.com
> **Cc:** O'Rourke, Allen (USADC) <AORourke@usa.doj.gov>; Kerkhoff, Jennifer (USADC) <JKerkhoff@usa.doj.gov>; christopher.ghazarian@dreamhost.com
> **Subject:** Re: Dreamhost - Preservation Request (LGL-53782)

Hi John,

Thank you for writing. It's looking like early next week at this point. We've had an usually large volume of issues for our team lately. We appreciate your patience in the meantime.

Sincerely,
Karl Fry
DreamHost Compliance Team
http://www.dreamhost.com

On 2/16/17 11:23 AM, Borchert, John (USADC) wrote:

> Hello, Karl - Can you give us a sense of where you stand with complying with the subpoena?
>
> Regards,
>
> John
>
> **From:** Karl Fry [mailto:karl.fry@dreamhost.com]
> **Sent:** Tuesday, February 14, 2017 6:17 PM
> **To:** Borchert, John (USADC) <JBorchert@usa.doj.gov>; legal@dreamhost.com
> **Cc:** O'Rourke, Allen (USADC) <AORourke@usa.doj.gov>; Kerkhoff, Jennifer (USADC) <JKerkhoff@usa.doj.gov>; christopher.ghazarian@dreamhost.com
> **Subject:** Re: Dreamhost - Preservation Request (LGL-53782)
>
> John,
>
> Thanks for writing. Yes, we were served by hand last week. It is in our queue for the week and I will get back to you as soon as I have more information. Thank you for your patience in the meantime.
>
> Sincerely,
> Karl
>
> On 2/10/17 10:14 AM, Borchert, John (USADC) wrote:
>
> > Hello, Karl - I believe you have now been served by hand. The effective preservation date should be January 27, which was the date of the preservation request. Please let me

know if you have any concerns complying with the subpoena.

Regards,

John

From: Borchert, John (USADC)
Sent: Thursday, February 2, 2017 1:15 PM
To: Karl Fry <karl.fry@dreamhost.com>; legal@dreamhost.com
Cc: O'Rourke, Allen (USADC) <AORourke@usa.doj.gov>; Kerkhoff, Jennifer (USADC) <JKerkhoff@usa.doj.gov>; christopher.ghazarian@dreamhost.com
Subject: RE: Dreamhost - Preservation Request (LGL-53782)

I understand how you plan to proceed.

From: Karl Fry [mailto:karl.fry@dreamhost.com]
Sent: Thursday, February 2, 2017 1:12 PM
To: Borchert, John (USADC) <JBorchert@usa.doj.gov>; legal@dreamhost.com
Cc: O'Rourke, Allen (USADC) <AORourke@usa.doj.gov>; Kerkhoff, Jennifer (USADC) <JKerkhoff@usa.doj.gov>; christopher.ghazarian@dreamhost.com
Subject: Re: Dreamhost - Preservation Request (LGL-53782)

John,

I will proceed with the preservation, but again -- we will have to notify our customer that we are preserving data since we are not compelled by a 2705(b) non-disclosure order. Please confirm that you understand we will be proceeding with notification.

The preservation will be effective as of Jan 28 if we proceed.

Karl

On 2/2/17 10:03 AM, Borchert, John (USADC) wrote:

> Karl –
>
> Please proceed with the preservation. The

preservation request was sent last week, so I assume that your preservation will be effective as of that date. Is that correct?

I understand your request regarding service and we are working on that.

Regards,

John

From: Karl Fry [mailto:karl.fry@dreamhost.com]
Sent: Thursday, February 2, 2017 12:51 PM
To: Borchert, John (USADC) <JBorchert@usa.doj.gov>; legal@dreamhost.com
Cc: O'Rourke, Allen (USADC) <AORourke@usa.doj.gov>; Kerkhoff, Jennifer (USADC) <JKerkhoff@usa.doj.gov>; christopher.ghazarian@dreamhost.com
Subject: Re: Dreamhost - Preservation Request (LGL-53782)

John,

Thank you for your patience on this issue.

After review, we've determined that in this case we would be required to notify our customer if we proceed with the preservation as our non-disclosure is merely requested and not required by law. Likewise, I should note, the subpoena you previously emailed us that we weren't able to comply with due to service-of-process issues did not include a 2705(b) non-disclosure order.

I will not notify our customer at this point unless you request us to proceed with the preservation without a valid 2705(b) non-disclosure order.

Also, if you do ultimately serve us with a production order, you'll likely want such a non-disclosure order attached if you do not want us to disclose to our customer.

Again I apologize for the time it took to review this issue. If you have any questions please let me know and I will expedite your request.

Thank you,
Karl Fry
DreamHost Compliance Team
http://www.dreamhost.com

On 1/29/17 11:03 AM, Borchert, John (USADC) wrote:

> Thank you very much. Please don't hesitate to reach out if you any questions.
>
> Regards,
>
> John
>
> John W. Borchert
> Assistant United States Attorney
> United States Attorney's Office for the
> District of Columbia
> Desk: (202) 252-7679
> Mobile: (202) 870-6071
>
> **From:** Karl Fry [mailto:karl.fry@dreamhost.com]
> **Sent:** Saturday, January 28, 2017 6:51 PM
> **To:** Borchert, John (USADC) <JBorchert@usa.doj.gov>; legal@dreamhost.com

Subject: Re: Dreamhost - Preservation Request (LGL-53782)

Thank you for writing.

I just wanted to let you know that we are in receipt of your preservation request and discussed it with our General Counsel on Friday. We will have further response for you on Monday. Thank you for your patience in the meantime.

Sincerely,
Karl Fry
DreamHost Compliance Team
http://www.dreamhost.com

On 1/27/17 10:54 AM, Borchert, John (USADC) wrote:

> Please see attached.
>
> John W. Borchert
> Assistant United States Attorney
> United States Attorney's Office for the
> District of Columbia
> Desk: (202) 252-7679
> Mobile: (202) 870-6071

EXHIBIT 3

ATTACHMENT B

Particular Things to be Seized

I. Information to be 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 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 the Account, including all files, databases, and database records stored by DreamHost in relation to that Account; AND

b. 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 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 HTTP request and error logs.

II. Information to be Seized by the Government

A. Description of the Evidence

The government may seize all information described above in Section I that constitutes evidence of the violations of D.C. Code §§ 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 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, 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 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.

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.