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

MEMORANDUM OF PROPOSED INTERVENORS DOE 6, DOE 7, AND DOE 8 OPPOSING ENTRY OF AN ORDER GIVING THE GOVERNMENT EVEN TEMPORARY ACCESS TO IDENTIFYING INFORMATION ABOUT INDIVIDUALS WHO SENT AND RECEIVED EMAILS TO AND FROM ADDRESSES ON THE DisruptJ20.org DOMAIN

TABLE OF AUTHORITIES

CASES

CONSTITUTION AND STATUTES

Introduction and Summary of Argument

This brief is addressed to a narrow category of the documents that the Government seeks pursuant to its search warrant: emails sent by members of the public to email addresses on the DisruptJ20.org domain; emails sent from email addresses on the DisruptJ20.org domain to members of the public; and lists of members of listservs maintained by the operators of the DisruptJ20 web site. The arguments are presented on behalf of three proposed Doe intervenors: members of the public who either sent such emails, or received such emails, or were members of the listservs, and who thus have standing to raise the constitutional issues presented in those respects; until this brief was filed, no counsel for such members of the public has been before the Court. The brief is based in part on facts that have come to light since the Court first addressed the Government's motion to show cause on August 24 (namely, defects in the affidavit supporting the search), and argues that the Court's order enforcing the search warrant should have due regard to the First Amendment protections for the anonymous speech and anonymous reading rights of such members of the public.

In this case, prosecutors working for the Trump Administration seek to take advantage of a prosecution directed at a number of individuals charged with premeditated violence against property and police officers, to conduct a raid on a set of electronic files representing communications from members of the public who contacted a web site in the interest of constitutionally-protected peaceful protest activities against that very Administration. The web site itself, to all public appearances, had nothing to do with plans for rioting or any other form of violence. Rather, it provided information about a wide range of activities being organized under the auspices of a number of different organizations, with the stated purpose of disrupting the inauguration of President Donald Trump by permitted demonstrations as well as protests involving "nonviolent direct action." The web site invited members of the public to contact the site's hosts to offer assistance and to provide email

addresses to which further information could be sent. The site's hosts accumulated lists of email addresses to which further information could be sent, for example, communications with the media or with lawyers and others who volunteered to help protect the legal rights of demonstrators.

Both the emails and the listserv membership lists contain information likely to identify the individuals who were in touch with the web site, inasmuch as an email address often includes the name of the addressee. Emails messages may well include identifying information, such as signature blocks, as well as sensitive and confidential information, such as legal advice. Once information about D.C. residents who regularly help demonstrators, and media sources who communicate about planned demonstrations, is seen by police officers and prosecutors, it will remain in their memories even if they are compelled to delete the documents containing it.

The probable cause affidavit is based primarily on assertions about information that the Government claims to have obtained though undercover investigations in January 2017, information to which members of the public who contacted the web site could not have had access and which could not, therefore, have impelled them to communicate with the web site to offer their assistance or to request updates with more information. This brief on behalf of three Doe Internet users who sent and received such emails, or who were members of the site's listservs, argues that the Court's adoption of the two-step procedure, even when constrained by the requirement of providing the Court with written justification for "seizing" particular documents, provides insufficient protection to the First Amendment interests at stake. The brief shows first that the affidavit supporting the search warrant does not, when read carefully and in light of the actual web site at issue (which can be viewed in its entirety on the Internet Archive), show the existence of probable cause to search emails sent by Internet users to accounts on the DisruptJ20 domain, emails sent from that domain

to Internet users who were not involved in creating the web site, and the lists of members of the listservs to which the operators of the web site sent mass emails.

The brief further explains the legal principles that require protecting both the identities of the Internet users who used email to interact with the web site and the contents of their emails. First, the First Amendment right to speak anonymously has been recognized by the Supreme Court and the D.C. Court of Appeals, and federal courts in the District of Columbia have recognized the right to read anonymously. Second, the D.C. Court of Appeals has required that notice be given to anonymous Internet users to so that they can appear to protect their anonymity **before** that right is taken away. Third, the federal Privacy Act limits government collection of records "describing how any individual exercises rights guaranteed by the First Amendment." 5 U.S.C. § 552a(e)(7). And fourth, the cases cited by the government for the application of a two-step process whereby the Government gets to **search** an entire database but may **seize** only those records needed to pursue its investigation or prosecution pertained generally to investigations of child pornography, money laundering and kickback schemes – none involved Government search of an intensely political web site devoted generally to peaceful opposition to the elected leader of that Government.

In these circumstances, the proposed intervenors urge the Court to balance the First Amendment interests of Internet users not involved in the creation of the DisruptJ20 web site by denying the government any access to the content of emails sent to the site or to the email addresses of those who sent such emails or received emails from the site, including the members of the email listservs. In the alternative, if that Court concludes that the Government had made a sufficient showing of probable cause with respect to some categories of emails, the Court order should adopt a modification of the two-step process—it could be called a three-step process—under which

DreamHost keeps sole possession of the emails and listserv memberships but allows the Government to have access to the content of emails in that category (with any identifying information removed), without putting those emails in the Government's possession. Only if the Government can explain to the Court's satisfaction why there is probable cause to believe that information identifying the senders or recipients of specific emails is needed to pursue the Government's prosecution of the individuals who allegedly participated in rioting on January 20, 2017, or who allegedly planned such rioting, should the Government be able to obtain those particular emails and, if the proper showing is made, the identifying portions of such documents.

Finally, in the event the Court rejects these arguments, the brief argues for a limited stay pending appeal, barring only the Government's access to emails and identifying information either pending an appeal on that issue or, at least, for long enough to give the D.C. Court of Appeals the opportunity to pass on the issue of a stay.

1. Because Government Has Not Shown Probable Cause to Believe that Emails Between Members of the Public and the Creators of the Site, or the Lists of Email Recipients, Would Contain Evidence of a Crime, Enforcement of the Warrant to Search Such Files Would Violate the Fourth Amendment.

It was only on the day of the Court's August 24 hearing on the Government's Motion to Show Cause that undersigned counsel learned that the affidavit filed in support of issuance of the search warrant had been made public, and only the following day that counsel obtained a copy of that affidavit. Although intervenors appreciate that the Court has ruled that the Government established probable cause to search documents pertaining to the web site in general, the Court has not, we believe, addressed the more specific question whether the Government has shown probable cause to search the narrow category of documents to intervenors' brief is addressed: emails sent between

users of the web site and email addresses on the web site's domain, and the lists of outsiders who were recipients of emails from listservs run by the web site. Intervenors argue in this section of the brief that the showing of need to search these documents in particular does not meet the test of "scrupulous exactitude." *See Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978), and hence that enforcement of the search warrant for these documents in particular would violate the Fourth Amendment. If nothing else, the weakness of the probable cause showing with respect to this sub-category of documents makes it all the more important that the Court balance the needs of the prosecutors to gain access to documents that would likely aid their effort to prosecute the alleged rioters against the First Amendment rights of outside speakers by denying prosecutors even preliminary access to documents identifying innocent speakers who did no more than communicate about plans for legally protected activity with email addresses on the DisruptJ20.org domain.

In that regard, the probable cause showing set forth in the supporting affidavit of Greggory Pemberton was misleading at best, and based on highly selective descriptions of the DisruptJ20 web site. Because the versions of the web site that were available online in December 2016 and January 2017 can be viewed on the Internet Archive, www.archive.org, the Court can see that the web site presented itself to the public as a resource for obtaining information about a wide range of protest events connected with the inauguration of Donald Trump during the long weekend of January 20, 21 and 22, both in Washington, DC and around the country. The DisruptJ20 home page linked to several pages within the DisruptJ20.org web site; various pages within the DisruptJ20 site listed events anticipated for Inauguration Weekend, and linked to a number of other web sites established by separate organizations that were running a variety of inauguration-related protests for which the umbrella group operating the web site provided general statements of support. The outside sites to

which the DisruptJ20 site linked included a several different web sites and Facebook pages of groups that were planning to demonstrate about particular issues at points near specific entrances to security-protected entrances to the Inauguration site. The outside organizations included the Democratic Socialist Alliance ("DSA"), the "Earth2Trump Roadshow," several counter-inaugural balls such as the Peace Ball, the UnNaugural, and the Unity Ball, the All In Service DC charitable initiative, as well as the January 21 Women's March and a number of other events. One of many advertised events was the "Anticapitalist+ Antifascist Convergence," which described its planned activities as being a black-clad "mobile bloc opposing capitalism and fascism," gathering at Logan Circle at 10 AM on January 20. As well as on DisruptJ20, this event was promoted on a page on the web site "itsgoingdown.org." https://itsgoingdown.org/fierce-anti- capitalist-anti-fascist-bloc-inauguration/. The web site at itsgoingdown.org describes itself as a platform for local groups of anarchists, https://itsgoingdown .org/about/; the page of the web site about the black-clad "convergence," although apparently posted in early January 2017, is still visible online at that location.

The Pemberton affidavit, ¶¶ 6-15, describes in great detail the January 20 riot activities of "an anarchist group," whose name he never discloses, involving a march beginning at Logan Circle at 10 AM. Paragraphs 16 and 17 of the affidavit are the only paragraphs that specifically discuss the DisruptJ20.org web site. Paragraph 16 asserts that "an anarchist group" planned and helped carry out the riot described in the previous paragraphs, and then asserts, without any supporting information, that "the group" created the Disrupt J20 web site as well as DisruptJ20 Twitter, Facebook, and Instagram accounts. Detective Pemberton never shows that he has personal knowledge of the identity of the people or "group" that created the DisruptJ20 web site, nor does he furnish any sworn statement providing a sound basis for concluding that the web site was organized

by the same "anarchist group" at whose feet he lays the planning of the alleged riot that forms the basis for the pending criminal prosecutions.

Paragraph 17 makes misleading statements about the connection between the advertised Logan Circle march and the DisruptJ20 web site. It states that a press release featured on the "media page" of the DisruptJ20 web site includes the sentence "An unpermitted, anticapitalist march will begin at 10 AM in Logan Circle." It also asserts that the "events" page on the DisruptJ20 web site linked to information about the "'Anticapitalist+Antifascist Convergence' event" planned to begin at 10 AM at Logan Circle. Although the DisruptJ20 site, as viewed on the Internet Archive, featured that event as one of many supported by the DC Counter-Inaugural Welcoming Committee, the media page linked that event to an **off-site** page with the detail "Wear all black | January 20th, 10 AM | Logan Circle, DC": https://web.archive.org/web/20170113163033/http://www.disruptj20.org/media/, linking to https://web.archive.org/web/20170113163342/https://itsgoingdown.org /fierce-anti-capitalist-anti-fascist-bloc-inauguration/. Counsel have not found a separate "events" page on the site; however, the home page included a "Schedule of Events" that also linked to the same page with the detail "Wear all black | January 20th, 10 AM | Logan Circle, DC". *See* https://web.archive.org/web/20170113162729/http://www.disruptj20.org//, linking to https://web.archive.org/web/20170113162921/https://itsgoingdown.org/fierce-anti-capitalist-anti-fascist-bloc-inauguration/?utm_content=buffer15f67&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer. Nor did the affidavit disclose that the Logan Circle gathering was one of dozens of events described on and linked from the DisruptJ20 media and home pages.

Finally, paragraphs 20 through 23 of the affidavit describe information obtained by an undercover police officer who attended two gatherings, but fails to connect the dots between the

statements at those meetings and either the DisuptJU20 web site or, more important, the perceptions of members of the public whose communications with the web site are now at issue. Paragraph 22 of the affidavit recounts statements by an individual named Dylan Petrohilos who discussed "the events planned for January 20," including statements about the march beginning at Logan Circle that strongly suggest that the infliction of property damage was contemplated. Paragraph 22 ties Petrohilos to DisruptJ20 (although not to the DisruptJ20 web site) by saying that Petrohilos had elsewhere identified himself as an "activist and organizer with the DisruptJ20 organization." Paragraph 21 of the affidavit says that, at a **different** meeting, the undercover officer "was required to log into a website on a computer." The affidavit does not identify the log-in web site. The Government's reply brief in support of enforcement of the warrant provided a misleading description of this part of the affidavit, claiming that the Government had shown that "the site was even used to verify the identity of people in closely-held meetings." Reply Brief in Support of Motion to Show Cause, page 2. In the context of that brief, the strong (but unsupported) implication was that "the site" referred to disruptJ20.org; but the affidavit does not make that specific connection.

Accordingly, there is some reason to question whether the Government has made a showing of probable cause to believe that there is **anything** about the DisruptJ20 web site that contains evidence of criminal intent on the part of the creators of the web site, or that will reveal planning for criminal activity. To the contrary, it appears that the DisruptJ20 site provided information about a large range of activities, almost all of them irrelevant to the riot for which the Government is prosecuting 200 people. Even if some individuals who belonged to the DisruptJ20 umbrella group were involved in the "anarchist group" described in the affidavit as having made plans for a riot, and even though the DisruptJ20 site connected to an advertisement for that group's planned black-clad

march, that scarcely provides probable cause to search all of the documents relating to the web site of the umbrella group.

Moreover, and more pertinent to the rights of the proposed intervenors, the purported showing of probable cause regarding the contents of email communications to and from the web site, and the need to identify outside Internet users, was particularly weak; it was more a matter of a wish and a dream than probable cause. The affidavits of the proposed intervenors, coupled with counsel's review of the site itself, identify six different email addresses and/or listservs—one for legal assistance, one for contact with the outside media, one for people hoping to provide medical assistance (medics@disruptj20.org), one for the "digital team," one for proposed issue-oriented demonstrations (action@disruptj20org), and one more general email address, info@disruptJ20.org. DreamHost may be able to specify other email addresses to and from which emails were sent, and other listservs whose members stand to be identified pursuant to the search warrant. The burden rests on the Government, in any event, to address those specifics in a showing of probable cause, and to do so with "scrupulous exactitude."

Rather than discussing evidence showing probable cause to believe that emails to or from specific addresses are likely to contain evidence of criminal activity unprotected by the First Amendment, paragraphs 19 and 24 of the affidavit—the **only** parts of the Pemberton Affidavit that even purport to support a finding of probable cause to search the emails—address this issue in highly conclusory terms. Paragraph 19 notes that the address info@disruptj20.org appears on the DisruptJ20.org web site as a place to get more information, and continues by speculating that the contents of communications such as RSVPs for housing and transportation might well "evidence the planning and coordination of the January 20, 2017 riot." In that regard, if the impression

misleadingly conveyed by the Pemberton affidavit that the DisruptJ20 web site was largely about the Black Bloc's march were correct, perhaps one could infer that emails about housing and transportation related to planning for participants in that march. But, as discussed above, the impression thus conveyed by the affidavit was misleading—the affidavit ignored the fact that the DisruptJ20 web site provided information about a large number of entirely peaceful events unrelated to the riot that is the subject of the Government's prosecution. Consequently, the contents of the affidavit, considered against the actual facts about the web site it was describing, never shows probable cause to believe that housing and transportation arrangements had anything to do with people arriving in Washington for the itsgoingdown-sponsored riot. Moreover, the affidavit does not even pretend to address a claimed need for access to emails directed to or from email addresses such as "legal@disruptJ20.org" or "media@disruptJ20.org."

Even more conclusory are fragments of the last two sentences of paragraph 24, which asserts, without any further support, that "the contents of . . . direct messages, . . . RSVP's and other communications likely contain evidence which may help to determine the intent, knowledge, and state of mind of the people who carried out the rioting activity. Further, the contents of communications . . . likely contain evidence helping to identify who organized and participated in the rioting activity." No basis is shown, apart from Pemberton's supposed expertise, for believing that this is true. Intervenors respectfully submit that such bare hope-and-dream predictions of what a search of the emails and listserv memberships might show is not the sort of "scrupulous exactitude" that the cases demand of search warrants affecting First Amendment interests.

As the U.S. Court of Appeals for the Fifth Circuit has said, "[i]t would be a sorry day were we to allow a grand jury to delve into the membership, meetings, minutes, organizational structure,

funding and political activities of unpopular organizations on the pretext that their members might have some information relevant to a crime." *Ealy v. Littlejohn*, 569 F.2d 219, 229 (5th Cir. 1978). *See also Fed. Election Comm'n v. Machinists Non-Partisan Political League*, 655 F.2d 380, 388 n.17 (D.C. Cir. 1981) ("One can only imagine what the Founding Fathers would have thought of a federal bureaucracy demanding comprehensive reports on the internal workings and membership lists of peaceful political groups.")

Moreover, the supposed showing of probable cause to search the DreamHost data is based in substantial part on the riotous activity that the Government's witnesses observed on January 20 —recited in paragraphs 7 to 15 of the affidavit—as well as information obtained from the attendance of an undercover officer at private meetings (¶¶ 20-23), and a podcast heard on a completely different web site, itsgoingdown.org (¶ 18). The affidavit contains no showing that people who visited the DisruptJ20 web site before January 20 were aware of its alleged connection to any anarchist group planning a riot, and no showing that visitors to the DisruptJ20 web site in the period leading up to January 20 had any occasion to learn that information. Hence there is no basis for inferring that those who communicated with email addresses on the web site, or who signed up for membership in the listservs, did so in an effort to help plan for a riot, or that there was any listserv that was related to planning for a riot. Consequently, there is no probable cause for extending the Government's search to the emails, to email addresses, and to listserv memberships. For this reason alone, the Court's order enforcing the warrant should exclude emails sent to addresses on the DisruptJ20 domain, emails sent to outside Internet users from email addresses on the DisruptJ20 domain, lists of members of listservs, and any other documents that disclose the identity of the outside Internet users who sent and received such emails.

2. On the Current Record, the First Amendment Bars Enforcement of the Search Warrant to Obtain Emails and Listserv Membership Lists.

Apart from the absence of probable cause sufficient to warrant the Government's search of emails between the web site operators and outside Internet users and of the listserv membership lists, which bars enforcement of the search warrant on Fourth Amendment grounds, the First Amendment provides an additional reason why the Government should not be given access to emails and listserv membership lists. Merely providing the Does' email addresses would likely identify them because email addresses commonly include the account owners' surnames and either their entire given names or part of the given names. Providing an email could also identify the sender if, as is commonly the case, the email contains a signature block; emails may also name names, as is the case for one of the Doe intervenors on whose behalf this brief is submitted. As that Doe's affidavit indicates, her email to legal@disruptJ20.org identified a different individual who had suggested to the Doe that she write to that email address to offer legal support services for the rights of demonstrators.[1]

The First Amendment protects against compelled disclosure of such identifying information. The brief filed on behalf of Does 1, 2, 3, 4, and 5 showed that the First Amendment guarantees a right to speak anonymously and to read anonymously, and that these rights can bar the enforcement of discovery to identify anonymous readers and speakers unless the Government shows a compelling interest in obtaining their information by showing evidence that the reading or speaking was wrongful. Memorandum at 4-8, citing such cases as *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341-42 (1995), and *Solers v. Doe*, 977 A.2d 941, 956 (D.C. 2009), on the right to speak anonymously, and *In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq.*,

[1] This memorandum uses female generic pronouns to identify Doe Internet users, without any intention of specifying the gender of such users.

706 F. Supp. 2d 11, 20 (D.D.C. 2009), and *In re Grand Jury Subpoena to Kramerbooks & Afterwords*, Inc., Nos. 98–MC–135–NHJ, 26 Med. L. Rptr. 1599, 1600 (D.D.C. Apr. 6, 1998), on the right to read anonymously. Moreover, as DreamHost has previously argued with respect to the lists of members of the DisruptJ20 listservs, the Supreme Court's decision in *NAACP v. Alabama*, 357 U.S. 449, 462 (1958), bars state action compelling the disclosure of membership lists of unpopular organizations absent a compelling interest requiring such disclosure. The record contains no evidence establishing any basis for believing that the various anonymous people who sent communications to email addresses on the DisruptJ20.org domain, or who asked that they be notified of developments about the impending January 20 protests (thus leading to the inclusion of their names in the listservs), were engaged in any criminal wrongdoing that warrants depriving them of the right to keep their communications anonymous. Nor is there any reason to believe that those who offered to provide legal support or medical assistance on January 20 were proposing illegal activity.

The previous brief that was filed on behalf of the proposed intervenor Does demonstrated that precedent in the District and elsewhere demands a substantive showing of wrongdoing before the right to remain anonymous can be taken away. Mem. at 4-5. In addition, the D.C. Court of Appeals has imposed procedural requirements before discovery is allowed to identify anonymous Internet speakers: a trial court "should require reasonable efforts to ensure that the Doe knows of the subpoena and has a chance to oppose it." *Solers v. Doe*, 977 A.2d at 954. Counsel for intervenors have urged DreamHost to use the email addresses that it can obtain from the listserv membership lists and from the emails themselves to give notice of the warrant to the Doe Internet users whose identities stand to be revealed, and have received no assurances on that score. Although Does 6, 7 and 8 learned of the search warrant without notice from DreamHost, but because of the efforts of

undersigned counsel, many other Does are likely unaware that their anonymity is threatened. Until such notice has been given, the Court should not place at risk the anonymity of members of the public who communicated with the web site.[2]

In support of its search warrant, the Government relied on a series of cases which, it contended, represent a consensus in favor of the application of a two-step process for the search of electronic information stored on computers or computer servers. Reply in Support of Motion to Show Cause, at 9-11. Pursuant to the two-step process, the Government is allowed to take possession of an entire set of electronic files for the purpose of "searching" them, that is, conducting a review to determine which of the files is relevant to its criminal investigation or prosecution. Through the search process, the Government identifies those electronic documents thus taken into the government's possession that are actually relevant to the investigation; the theory is that only the relevant files are "seized." But the cases on which the government relies are very different from this one. The great majority of the cases involved child pornography investigations, in which courts have had to weigh the privacy interests of files typically stored on the computers of people who are the targets of child pornography investigations against the strong public interest in fighting the scourge of child pornography. A handful of other cases involved investigations of kickback schemes and money laundering, in which the privacy interests at stake were largely commercial. Not one of the Government's cases involved a search of the files connected to a political web site dedicated to opposing, by nonviolent means, the head of the Government whose agents are conducting the search.

[2] In the interim, while the notice is being sent and the Does are being given time to find their own counsel, the Court might consider appointing counsel ad litem to protect the anonymity interests of the Does other than the three represented by undersigned counsel, as a judge of the United States District Court for the Northern District of Texas did in *Mick Haig Productions v. Doe*, 687 F.3d 649 (5th Cir. 2012).

The Court should be very cautious about the precedent that its order in this case will set, allowing prosecutors working for a President with a well-documented history of intolerance of political opposition, lack of respect for opponents' free speech rights, and willingness to encourage his supporters to beat up peaceful protesters, to search the electronic files of opposition groups on a minimal showing of probable cause. Particularly in this context, the very fact of searching the entire set of emails sent to a web site putatively promoting nonviolent protest, sweeping into the government's net the identities of people not connected to the web site who did no more than communicate to try to obtain more information or to offer nonviolent support, will inevitably have a serious chilling effect that offends the First Amendment. *See NAACP v. Alabama*, 357 U.S. 449, 462 (1958); *In re Grand Jury Subpoena to Amazon.com Dated Aug. 7, 2006*, 246 F.R.D. 570, 572 (W.D. Wis. 2007).

Moreover, in contrast to the two-step process commonly employed in child porn and money laundering investigations, where political speech is at issue, the Privacy Act of 1974 points in a very different direction. That statute "safeguards the public from unwarranted collection, maintenance, use and dissemination of personal information contained in agency records." *Bartel v. FAA*, 725 F.2d 1403, 1407 (D.C. Cir. 1984). Toward that end, section (e)(7) of the Privacy Act prohibits any "agency"—a term that includes the United States Attorney's office—from maintaining any "record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7). The word "maintained" as defined by the statute "includes maintain, collect, use, or disseminate," and the caselaw is clear that the prohibition in section 552a(e)(7) is not limited to keeping records within the

government's files—in this context, the "seizure" stage of the two-step process. Even collecting the information in the first place—in this context, taking possession of the files for the purpose of searching them—is forbidden unless one of the narrow statutory exceptions applies. *Albright v. United States*, 631 F.2d 915, 919 (D.C. Cir. 1980) ("an agency may not so much as collect information about an individual's exercise of First Amendment rights" absent a statutory exception).

This prohibition reflects the concern, long recognized by the courts, that "the First Amendment has a penumbra where privacy is protected from governmental intrusion," and that "[t]his penumbra of privacy can be invaded, under certain circumstances, by the mere inquiry of government into an individual's exercise of First Amendment rights." *Albright v. United States*, 631 F.2d 915, 919 (D.C. Cir. 1980) (citation omitted). "Thus it is not surprising that Congress would have provided in this Act, dedicated to the protection of privacy, that an agency may not so much as collect information about an individual's exercise of First Amendment rights except under very circumscribed conditions." *Id.*

Here, the Government relies on the law enforcement exception to section 552a(e)(7), but that exception does not protect the execution of this search warrant to the extent that the warrant commands delivery of all emails and listserv membership lists. The law enforcement exception requires that the files be **both** "pertinent to **and** within the scope of" the law enforcement activity. Section 552a(e)(7) (emphasis added). Even assuming that these files are "within the scope of" the Government's enforcement of the criminal laws against individuals charged with rioting, the Government has not established that the files are "pertinent to" that prosecution. To the contrary, the Court's requirement that the Government provide a written, reasoned explanation justifying the relevance of a given file to its legitimate prosecutorial efforts is the process whereby the Government

may attempt to show the "pertinen[ce]" required by the Privacy Act. But, until that showing has been made, and approved by the Court, pertinence has not been established and the Government should not be allowed to take even temporary possession of the files.[3]

Accordingly, the Court should not allow the Government to proceed to obtain email or listserv files unless it shows probable cause to believe that **those** files contain evidence needed for its prosecution. The Court should require such as probable cause showing to be made for emails to and from particular email addresses on the DisruptJ20.org domain, and for particular listservs. Although, on the present record, intervenors do not believe that a probable cause showing has been made for any emails exchanged with outsiders, or for any listservs, it seems likely that the case for probable cause may be especially hard to make with respect to some subjects, such as emails to and from the email addresses "legal@disruptJ20.org," "medics@disruptJ20.org," or "media@disruptJ20.org," or for any listservs associated with those subjects.

Assuming that a probable cause showing can be made with respect to any particular DisruptJ20 email address or listserv, and assuming further that the Court approves the Government's search formula, using the process described on August 24, the Government's review should be required to proceed in stages. DreamHost should be required to maintain its database for inspection at a location in Washington, D.C., where it is more convenient for the prosecutors. For example, the law firm representing DreamHost, Kilpatrick Townsend & Stockton LLP, has a D.C. office that might provide a convenient venue for the review of the email and listserv files. Those files for which

[3] DreamHost argues that the proposed order should provide that the Government will not be allowed to proceed along the stages of the two-step process unless and until the Court approves the Government's proposed search plans and its justifications for "seizing" specific files. Intervenors agree that the requirement of approval **before** further search or seizure was implicit in the Court's directions.

a general probable cause showing had been made should be made available for inspection with any identifying information redacted. Only if the Government can make a showing, satisfactory to the Court, that the contents of a particular email or particular listserv message contains information needed for its prosecution, should the Government be allowed to obtain possession of that email. And only if the Government shows to the Court's satisfaction that the identity of the sender or recipient of that email (or other identifying information contained within the email) is needed for its prosecution, should the Government be given access to that information as well.

The briefs of the Government and DreamHost disagree about whether the Government's showings in support of its claims to "seize" particular files should be made ex parte or with an opportunity for opposition by DreamHost; the same question would be presented were the Court to adopt the three-step process here proposed by intervenors. In that regard, the Court should give maximum opportunity for the adversarial process to develop facts and arguments for its review. Our system of justice depends on the adversarial process to produce just results. Counsel fully recognize and appreciate the burdens that the Court has assumed in agreeing to review the Government's document-specific showings. However, there is every reason to anticipate that, just as discussions between counsel for DreamHost and the Government were able to narrow the disputes about particular language issues in the proposed order, employment of the adversarial process to develop arguments for and against the disclosure of particular emails or particular email addresses may well reduce the number of documents that the Court will be required to review.

And, in that regard, there is no reason why the Government should not be required to make showings in support of its demand for the privilege of reviewing the files of its political opponents in full public view. If information from certain filings needs to be redacted to protect the privacy

of third parties, the Government, as well as DreamHost and appointed or retained counsel for the Does, should be allowed to file unredacted papers under seal. At the same time, the adversarial process proposed by intervenors ensures the development of a good record for any appeal that might eventuate, not to speak of a record that can help the public assess, after the fact, whether the judicial process has afforded sufficient protections for the First Amendment rights of dissenters against invasion by agents of the Administration.

3. If the Court Rejects Intervenors' Arguments for Further Protections for the Identities of Anonymous Internet Users Who Communicated with the DisruptJ20 Web Site, It Should Grant a Limited Stay Pending Appeal.

DreamHost has urged the Court to grant a general stay of its enforcement of the search warrant pending appeal; the Government has signaled its opposition although it also said that the issue is premature because the Court has not yet issued any enforcement order, and that any showings on a stay should only be made once such an order is issued.

> To prevail on a motion for stay, a movant must show that he or she is likely to succeed on the merits, that irreparable injury will result if the stay is denied, that opposing parties will not be harmed by a stay, and that the public interest favors the granting of a stay. *Barry v. Washington Post Co.*, 529 A.2d 319, 320-21 (D.C.1987). These factors interrelate on a sliding scale and must be balanced against each other. *Serono Labs., Inc. v. Shalala*, 158 F.3d 1313, 1318 (D.C. Cir.1998).
>
> *Salvattera v. Ramirez*, 105 A.3d 1003, 1005 (D.C. App. 2014).

Thus, a party "need not show a mathematical probability of success on the merits." *Akassy v. William Penn Apartments Ltd. P'ship.*, 891 A.2d 291, 310 (D.C. 2006). Rather, "[a] stay may be granted with either a high probability of success and some injury, or vice versa. . . . Thus, if irreparable harm is clearly shown, the movant may prevail by demonstrating that he or she has a substantial case on the merits." *Id.*

Intervenors submit that, to the extent that the Court's order allows the Government to obtain identifying information about members of the public who communicated with the DisruptJ20.org domain, or whose identifying information would be disclosed by seizure of the lists of members of email listservs, the case for a stay pending appeal is compelling. Once the names of political opponents who communicated with the DisruptJ20.org web site are disclosed, their anonymity can never be restored. It is for that reason that trial court orders enforcing discovery to identify anonymous Internet speakers have typically been stayed pending appellate review. *Doe No. 1 v. Burke*, 91 A.3d 1031, 1042 (D.C. App. 2014); *In re Indiana Newspapers*, 963 N.E.2d 534, 542 (Ind. App. 2012); *Indep. Newspapers, Inc. v. Brodie*, 966 A.2d 432, 447 (Md. 2009); *Doe v. Cahill*, 884 A.2d 451, 455 (Del. 2005).

The Government's strongest argument against the stay is likely to be that the trials of the defendants charged in connection with the January 20 riot are scheduled to begin this fall. However, **none** of the delay in putting this matter in the Court's hands for decision is due to failures of the intervenors, who sought leave to participate in the search warrant litigation within days of learning that their First Amendment right to anonymity was threatened. The Government, by contrast, did not seek issuance of the search warrant until mid-July, even though its purported showing of probable cause is based entirely on facts that were within the Government's knowledge on or before January 20, 2017, and even though its initial demand for documents from DreamHost was issued on January 27. The Government has never explained the six-month delay in securing the search warrant; if the process of adjudicating the validity of compelled production of a small fraction of the documents within the broad sweep of the warrant is pressing the Government up against its trial deadlines, it has only itself to blame.

Moreover, in seeking a limited stay pending appeal, intervenors stand ready to seek and cooperate in expedited appellate processing including, possibly, an early review by the Court of Appeals of the question whether the stay should be maintained pending completion of the appeal. Indeed, if nothing else, the Court should grant a stay sufficiently long in duration to give intervenors a fair opportunity to seek a stay from the Court of Appeals.

CONCLUSION

The Court's order should exclude emails sent to email addresses on the DisruptJ20,org domain from members of the public, emails sent from email addresses on the DisruptJ20.org domain to members of the public, and the list of emails of people belonging to the DisruptJ20 listservs, from the categories of documents required to be provided pursuant to the search warrant. To the extent that the Court does not exclude those classes of documents from the warrant entirely, it should adopt the three-step process allowing a search of those documents as proposed in the foregoing brief. Finally, to the extent that any of these exceptions is not adopted, the Court should grant a limited stay pending appeal.

Respectfully submitted,

/s/ Paul Alan Levy

Paul Alan Levy (D.C. Bar 946400)
Adina Rosenbaum (D.C. Bar 490928)

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

September 7, 2017

Attorneys for Doe Movants

CERTIFICATE OF SERVICE

I hereby certify that, on this 7th day of September, 2017, I will serve copies this memorandum both by first-class mail and by email on counsel for the Government and counsel for DreamHost, as follows:

Raymond O. Aghaian, Esquire
Kilpatrick Townsend & Stockton LLP
9720 Wilshire Blvd
Beverly Hills, California 90212-2018
raghaian@kilpatricktownsend.com

Chris Ghazarian, Esquire
DreamHost
Suite 5050
707 Wilshire Blvd
Los Angeles, California 90017
chris@dreamhost.com

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

/s/ Paul Alan Levy
Paul Alan Levy

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