



September 7, 2017

The Honorable Robert E. Morin
Chief Judge
Superior Court of the District of Columbia
500 Indiana Ave. NW
Washington, D.C. 20001

Re: *In the Matter of the Search of www.disruptj20.org that is Stored at Premises
Owned, Maintained, Controlled or Operated by DreamHost*

Special Proceedings Nos. 17-CSW-3438

Dear Chief Judge Morin:

I write on behalf of the Electronic Frontier Foundation (“EFF”) regarding the above-captioned matter and in support of an order that protects the vital liberty interests at stake in this case.

EFF is a non-profit civil liberties organization dedicated to protecting and promoting civil liberties in the digital age. EFF often serves as amicus in the District of Columbia and in courts across the country in cases that implicate constitutional rights in the digital age. *See, e.g., Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017) (citing EFF amicus brief).

The government’s investigation into www.disruptj20.org—a website dedicated to planning a series of protests on the day of President Trump’s inauguration¹—raises serious concerns that cut to the heart of the protections afforded by the First and Fourth Amendments. These concerns stem from the government’s demand that the website’s hosting provider, DreamHost, turn over a broad swath of information concerning individuals that operated and communicated with the site. Although the government’s decision to narrow the scope of the warrant obviates some of the warrant’s constitutional defects, it has not cured them entirely.

¹ Having reviewed the affidavit submitted in this matter, EFF believes it contains a series of material omissions that create the implication that the website was dedicated solely to coordinating the so-called “Anticapitalist+Antifascist Convergence”—the protest that the government alleges devolved into a riot. What the government conspicuously omits, however, is that the “Convergence” was just one of a *series* of protests—none of which are alleged to have become violent—that occurred on Inauguration Day and that were organized through the disruptj20.org site. These omissions bear on both the likelihood that the search will uncover information necessary to the investigation and the breadth of the search, should it ultimately be authorized.

In light of the significant constitutional concerns at issue here, we write to urge the Court to impose limitations on the government’s ability to search and seize data from DreamHost—limitations that other courts, in analogous contexts, have recognized as necessary to protect the important rights at issue in this case.

As explained in more depth below, EFF supports the safeguards contained in the proposed order, as submitted by DreamHost, and encourages the Court to impose additional limitations on the government’s handling of the data.

* * *

The First Amendment concerns present here are neither abstract nor ancillary. Rather, the government’s investigation of this site—one dedicated to coordinating and planning political protests—implicates a cross-section of critical First Amendment protections: the right to engage in political protest and dissent, *Tinker v. Des Moines Independent Community School District*, 393 U.S. 503 (1969); the right to associate, *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958); and the right to distribute and receive information, including the ability to do so anonymously. *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334 (1995); *Lamont v. Postmaster Gen.*, 381 U.S. 301, 307 (1965).

When government investigations raise significant First Amendment concerns such as these, courts have imposed heightened requirements, akin to strict scrutiny, before allowing the investigation to proceed. *See, e.g., Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1057 (Colo. 2002); *In re Grand Jury Subpoena to Kramerbooks & Afterwords Inc.*, 26 Media L. Rep. 1599, 1599-1601 (D.D.C. 1998); *Amazon.com LLC v. Lay*, 758 F. Supp. 2d 1154, 1168 (W.D. Wash. 2010); *In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461*, 706 F. Supp. 2d 11, 18-19 (D.D.C. 2009).

In perhaps the best-known example, the Colorado Supreme Court found that a warrant seeking a bookstore’s customer records implicated the “fundamental right to purchase books anonymously, free from governmental interference” and that “the book-buying records of innocent customers [would] almost inevitably be exposed to governmental observation.” *Tattered Cover*, 44 P.3d at 1047, 1060. As a result, the court held that the government needed to articulate a “compelling need *for the precise and specific information sought*” and that this need must outweigh the corresponding harm to First Amendment rights. *Id.* at 1058-59 (emphasis in original).

Similar consideration for the First Amendment is necessary here. Even after narrowing, the information responsive to the warrant will certainly include wholly innocent, First Amendment-protected communications. The government should not gain access to this information in the first place.

The First Amendment concerns coexist in this case with the significant Fourth Amendment concerns that arise in many cases involving digital search and seizure. That is: law enforcement obtains a warrant that authorizes the seizure and search of large volumes of unresponsive data—data that, in this case, implicates individuals’ core First

Amendment rights. Under these circumstances, the government’s proposed search procedures must be narrowed to adhere to the Fourth Amendment with “scrupulous exactitude.” *Zurcher v. Stanford Daily*, 436 U.S. 547, 554 (1978).

Courts have recognized that this problem—the “overseizure” of unresponsive data—risks “turning a limited search for particular information into a general search,” which the Fourth Amendment prohibits. *United States v. Comprehensive Drug Testing, Inc.* (“CDT”), 621 F.3d 1162, 1170 (9th Cir. 2010) (en banc); *see also United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (risk of digital searches becoming too general “demands a heightened sensitivity to the particularity requirement in the context of digital searches”).

Indeed, digital searches can be even more intrusive than a search of a person’s home, as the Supreme Court’s decision in *Riley v. California*, 134 S. Ct. 2473 (2014), recognizes: an electronic device “not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form.” *Id.* at 2491; *see also id.* at 2489 (describing types of sensitive data found on electronic devices).

To help mitigate the risk posed to Fourth Amendment rights by digital searches, courts have imposed restrictions and protocols on the execution of government searches and seizures. For example, in *CDT*, Judge Kozinski, in a concurring opinion joined by four other judges, offered specific guidance for how judges should impose ex ante search conditions to ensure digital searches remain tailored to evidence for which the government has probable cause. *See id.* at 1178 (Kozinski, J., concurring).

These conditions include: (1) forswearing reliance on the “plain view” doctrine;² (2) mandating the use of an independent third party or special master to conduct the forensic analysis; (3) requiring the government to disclose actual risks of destruction and other avenues of accessing information to the court; (4) judicial oversight of a search protocol “designed to uncover only the information for which [the government] has probable cause;” and (5) a minimization plan that requires the destruction or return of any non-responsive data beyond the scope of the warrant. *Id.* at 1180.

EFF supports the protections included in the proposed order submitted by DreamHost, including the limitation on the government’s ability to search data pending resolution of DreamHost’s appeal,³ and the parties’ jointly proposed requirement that the government

² The plain view doctrine allows an officer who is lawfully present in a place to seize an item if its illegal nature is “immediately apparent.” *Horton v. California*, 496 U.S. 128, 136-37 (1990). It is not clear how the plain view doctrine should apply in the context of digital searches, if at all. *See CDT*, 621 F.3d at 1171.

³ EFF believes a stay is particularly appropriate in light of the constitutional infirmity of some aspects of the proposed order. In particular, the government apparently seeks disclosure of the contents of multiple email accounts with a single warrant, as well

destroy any non-responsive data after completion of its search. However, EFF urges the Court to impose additional restrictions, including, but not limited to, those described above. In particular, EFF encourages the Court to appoint a special master or independent third-party to review information produced by DreamHost and to assess its responsiveness to the warrant, in lieu of production directly to the government.

* * *

The safeguards proposed above will help protect the significant First and Fourth Amendment rights implicated by the government's investigation of this website.

Respectfully,



David L. Sobel
(D.C. Bar # 360418)
ELECTRONIC FRONTIER FOUNDATION
5335 Wisconsin Ave., N.W. Suite 640
Washington D.C. 20015
(202) 246-6180

Mark Rumold
Stephanie Lacambra
Nate Cardozo
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333 x137

cc: by email

Alysa Pfeiffer; Alysa.Pfeiffer@dcsc.gov
John Borchert; John.Borchert@usdoj.gov
Jennifer Kerkhoff; Jennifer.kerkhoff@usdoj.gov
Raymond Aghaian; RAghaian@kilpatricktownsend.com
Chris Ghazarian; christopher.ghazarian@dreamhost.com
Paul Levy; plevy@citizen.org

as the production of “subscriber lists” and other identifying information for those visiting or involved with the website. Both aspects of the warrant raise constitutional questions, *see, e.g., NAACP*, 357 U.S. at 459 (barring compelled production of NAACP membership lists)—questions that the Court of Appeals should have an opportunity to resolve before the government may access the data.