ON THE DREAMHOST WARRANT

You've probably already read about DOJ's expansive request for information on the website Disrupt J20 via a warrant served on its host, DreamHost. The information the government has asked for would cover the browsing records of 1.3 million visitors to the Disrupt site. After DOJ served the warrant on July 14, DreamHost challenged it. On July 28, DOJ asked a court to force DreamHost to turn over the records. On Friday, DreamHost responded, laying out why they believed the request to be overly broad. DreamHost's post on the challenge yesterday has generated a good deal of coverage.

Before I get to the breadth of the request, consider the background. The demand comes in the context of DOJ's efforts to prosecute 200 people who participated in protests on inauguration day. While there was definitely violent destruction associated with the protests, there have been numerous reports of entirely peaceful protestors being included in the 200, including journalists.

The timing and the urgency with which DOJ is seeking the information (see the emails included in this filing) make me wonder whether this is a desperate attempt to sustain another overly broad effort, to prosecute both peaceful and violent protestors of the President. Is DOJ preparing to argue that people who accessed information via Disrupt J20, which it has associated with "a riot," must themselves be rioters?

Note, too, that among the information DOJ will receive if this warrant is honored, is information posted on the site on how people charged might seek legal help, including emails pertaining to that section of the site. In other words, DOJ is seeking, in part, information on how people it has charged will respond to being charged (though I'm not claiming this amounts to

attorney-client privilege).

It's against that background that the breadth question gets interesting, in my opinion.

Orin Kerr argues that the warrant may not be problematic because the second step of the search would provide particularity — a focus on actual rioters — after DreamHost has turned over the information.

> [I]t's not obvious to me whether the warrant is problematic. Attachment B tells Dreamhost to turn over records to the government relating to "each account and identifier listed in Attachment A." Notably, Attachment A doesn't list any specific *user* accounts: It just lists the specific *website*. So the warrant seems to be telling Dreamhost to turn over pretty much everything it has on that website. I understand this to be Dreamhost's objection. Dreamhost thinks the warrant should only require it to hand over specific records about specific users.
>
> What makes this tricky, I think, is that Dreamhost is only involved in the initial search stage of a two-stage warrant. Computer warrants are ordinarily executed in two stages. First, the government gets access to all the electronic records. Next, the government searches through the records for the particularly described evidence. Courts have broadly allowed the government to follow this two-step procedure, in which they get all the stuff in the initial stage of electronic evidence warrants so that they can search it for the relevant evidence. Given that, Dreamhost's objection is slightly off. As I read it, Dreamhost is essentially challenging the widely accepted two-stage warrant practice. Some federal magistrate judges in the "magistrate's revolt" have made that

> argument, but they generally have been overruled at the district court level.

But DreamHost argues that the description of that second stage doesn't provide particularity at all, not least because after laying out some seeming limiting language, the warrant then asks for "files, databases, and database records" — that is, everything.

> The Search Warrant's description of the things to be seized does not pass the particularity test. It defines what is to be seized in three ways. First, it is information that "constitutes fruits, evidence, and instrumentalities of violations of" the rioting statute "involving the individuals who participated, planed [sic], organized, or incited the January 20 riot." Second, the information "relat[es] to the development, publishing, advertisement, access, use, administration or maintenance of" the website. Third, the information to be seized includes "files, databases, and database records." Yet, describing the information to be seized as evidence of a crime "involving" unnamed participants in the crime does not provide any meaningful specificity. Compare Apple, 13 F. Supp. 3d at 161 (description of things to be seized identified the information as "involving any or all of the following: [individuals and entities . . .]"). Limiting the information seized to that "relating to" the "publishing" or "use" of the website also lacks the required specificity, since practically any conceivable information about a web site is related to its publishing or use. Similarly, even if the use of the term "including" after the preceding broad description imposed some limit on the information to be seized, which it does not, limiting

> the seizure to electronic “files, databases, and database records” is no limit at all. Finally, the lack of a date range alone fails the specificity test. See Microsoft, 212 F. Supp. 3d at 1036 (“In cases in which courts have either denied a search warrant for the entirety of an email account or suppressed evidence based on an overbroad search warrant, the warrants lacked particularity, for example, in identifying a specified date range . . . .”).

Paul Ohm raises a number of interesting points in this thread, ultimately arguing that the warrant should go to the site administrators, not to DreamHost.

> This is less like a warrant to Gmail and more like one to Amazon Web Services. The warrant should go to the site admins, not @DreamHost

He also notes that the only reason the entire database for this period is intact is because the government got a preservation order using a 2703(f) preservation letter, which didn’t require any due process.

I want to add just one more point to this.

The breadth of this request is the kind of thing the government does in the national security context — they did with the phone and Internet dragnet, and probably intend to do more of if and when they get the right to obtain Electronic Communications Transaction Records via an NSL. The prosecutor, John Borchert, has prosecuted NSD cases in the past. As such, it’s worth asking whether DOJ is really treating this “riot” as a national security case, with even further chill on those who actually just protested (or in the case of journalists, reported on a protest). The debate on whether or not obtaining all the search records for a site

is overbroad may well constrain what the government can do, in secret, in the name of national security.