SUPERIOR COURT OF THE DISTRICT OF COLUMBIA
CRIMINAL DIVISION — SPECIAL PROCEEDINGS

In the Matter of the Search of Information Associated with Facebook Accounts disruptj20, lacymacauley, and legba.carrefour That Is Stored at Premises Controlled by Facebook, Inc.	)))))	Special Proceedings Nos. 17-CSW-658, 17-CSW-659 & 17-CSW-660 Chief Judge Morin

MOTION OF INTERVENORS TO QUASH OR NARROW SEARCH WARRANTS

TABLE OF AUTHORITIES

*Authorities on which we chiefly rely are marked with an asterisk.

Cases

Constitutional Provisions, Statutes and Rules

Other Authorities

INTRODUCTION

Three political activists have intervened in this matter to ask this Court to quash — or in the alternative, narrow — search warrants that would force Facebook to disclose to the government the entire contents of their Facebook accounts for a period of approximately 90 days. The warrants are manifestly overbroad. Most of the material demanded bears no relation to the government investigation for which the government sought the warrants. The government purports to seek to "seize" only the materials related to its investigation, yet the warrant requires that the entire contents of the target accounts be "disclosed" to the government. Permitting government officials to comb through 90 days' worth of personal messages concerning political activity and associations — some of which are aimed at protesting the policies of the very administration on whose behalf the government officials would be acting in searching Intervenors' records — is an unjustified invasion of privacy hearkening back to the "general warrants" that the Fourth Amendment was enacted specifically to prohibit. Additionally, the enforcement of the warrants would chill future online communications of political activists and anyone who communicates with them, as they will learn from these searches that no Facebook privacy setting can protect them from government snooping on political and personal materials far removed from any proper law enforcement interest.

The Intervenors recognize the need to sort relevant from irrelevant information in the context of an electronic search. But given the absence of any safeguards or minimization procedures in these warrants, the government will be free to peruse all the Intervenors' Facebook content at whatever level of detail and using whatever search tools they wish on their way to finding the material that is the reason for the search. Particularly where, as here, First Amendment concerns regarding political association are implicated, the absence of procedural safeguards renders the warrants fatally defective under the Fourth Amendment. The Court should quash the

warrants, or at a minimum narrow them by imposing procedural safeguards adequate to protect the fundamental associational and privacy interests at stake.

STATEMENT OF THE CASE

On January 20, 2017, Donald J. Trump was sworn in as President of the United States. Exercising their constitutional right to freedom of speech and assembly, people from all over the country took to the streets of the nation's capital to express their disapproval of his positions. During the course of demonstrations in the District of Columbia that day, several acts of vandalism occurred. In response, the District's Metropolitan Police Department rounded up and arrested hundreds of people. Ultimately, the government charged nearly everyone swept up by the police — more than 200 people — with a variety of D.C. Code offenses, including various offenses involving "rioting" or inciting "riots." D.C. Code § 22-1322.

On February 9, 2017, the government obtained from this Court the three search warrants at issue here for three Facebook accounts — the *disruptj20* Facebook page (owned by Intervenor Emmelia Talarico), and the personal accounts *lacymacauley* (owned by Intervenor Lacy MacAuley) and *legba.carrefour* (owned by Intervenor Legba Carrefour). These warrants require that, for each account, a trove of information "be disclosed by Facebook" to the government. Search Warrants Nos. 17-CSW-658, -659 & -660 ("Search Warrants"), Attachment B, at 1 (attached to this motion as Exhibit A). The information demanded pertained to the time period from November 1, 2016, to "the present" (i.e., February 9), and can be classified in two categories. One category is transactional information: all identifiers for devices used to access the account, records of session times and durations, length of service and payment records, privacy settings, subscriber records for all other Facebook accounts linked to that account, and communications with Facebook about the account. *Id.* at 1-2, items (b), (c), (d), (l), (m), & (n). The other category

is personal content: the user's personal identifying and security information (including password and security question information, home addresses, and credit card numbers), posts and activity logs, information about the use of any Facebook applications, photos and videos on the account, data deleted by the user, which other users the user has blocked, and three expansive subcategories of communications and associative information: "All electronic communications and messages, including direct messages, chats, video calls, live streams, and Facebook Messenger communications"; "All records of Facebook searches performed by the account"; and

> All profile information; News Feed information; status updates; links to videos, photographs, or other web content; Notes; Wall postings; Comments; Friend lists, including the friends' Facebook user ID numbers; groups and networks joined by the Account, including the Facebook group ID numbers; event postings; and pending and rejected "Friend" requests.

Id. at 1-2, items (a), (e), (f), (g), (h), (i), (j) & (*l*). In short, the warrants sought a complete record of anything the three users communicated or received from a third party via Facebook, everyone with whom the users associated via Facebook, and everything the users searched for on Facebook, during the specified time period.

The warrants went on to designate the subset of the "disclosed" information to be "seized" by the government; this subset consists of communications about the alleged "riot activity" on January 20 "leading to arrests at or near the intersection of 12th and L Streets, NW, in Washington, DC"; information about "perpetrators" and other "conspirators" in the alleged "riot"; information about the state of mind of the account owners and any "riot" participant with respect to the alleged "riot"; information about planning or covering up the alleged "riot"; information about actual or anticipated property damage; geographic and temporal information about account access that could "determine the geographic and chronological context of account access, use, and events pertaining

to the criminal activity under investigation and to the owner of the Account"; and the identity of the accounts' users and creators. *Id.* at 4-5.

The Facebook accounts at issue contain a significant quantity of non-public information, unrelated to the items that the government is authorized to "seize," that is deeply personal and/or pertains to the exercise of constitutional freedoms of speech and association by the owners of the targeted Facebook accounts, their friends and associates, and the thousands of individuals who merely indicated that they "liked" the disruptj20 Facebook page or planned to attend an event sponsored by that page. *See* Decl. of Emmelia Talarico (attached as Exhibit B), at 2 (estimating that 6,000 individuals "liked" the page prior to February 9, 2017). Despite their irrelevance to the government's investigation and to the stated purpose of the warrants, these categories of personal and associational/expressive information must be disclosed to the government under the terms of the warrants. The warrants make no provision for avoiding or minimizing invasions into personal and associational/expressive information, for preventing such information from being shared widely within the government, or for destroying irrelevant material when the investigation is concluded.

The enforcement of these warrants would reach deeply into individuals' private lives and protected associational and political activity. Government agents would gain access to the Intervenors' communications with friends and family members, and pictures and names of their family members, including the pictures and names of minor children and pictures of an Intervenor's child relatives in the bath. *See* Decl. of Lacy MacAuley (attached as Exhibit C), at 1; Decl. of Legba Carrefour (attached as Exhibit D), at 1. The government would come into possession of personal passwords, security questions, home addresses, and/or credit card information. *See* Decl. of Emmelia Talarico, at 1; *see also* Search Warrants, Attachment B, at 1,

items (a) & (d). The government would be able to read messages of a deeply personal nature, including intimate messages exchanged between an Intervenor and a romantic partner, an Intervenor's medical information including prescription-drug information and psychiatric history and treatment, and detailed discussions of an Intervenor's and third-parties' experiences with domestic violence. *See* Decl. of Lacy MacAuley, at 1; Decl. of Legba Carrefour, at 1. The government would see death threats received by an Intervenor that refer to specific traumatic incidents from her life. *See* Decl. of Lacy MacAuley, at 1.

Government agents would discover a detailed portrait of Intervenors' and third parties' political activities and associations. The government could read posts reflecting Intervenors' political views and commentary, including advocacy regarding how to vote in the 2016 Presidential election, and strings of posts in which third parties express their own political views and commentary. *See* Decl. of Lacy MacAuley, at 2; Decl. of Legba Carrefour, at 2. The government would see advertisements for and accounts of political demonstrations, rallies, dance parties, teach-ins, and other events in which many Facebook users participated and that had no connection to any alleged "riot" in the District of Columbia on January 20 (including many events that did not take place in the District of Columbia, did not take place on January 20, or were unrelated to the inaugural ceremonies). *See* Decl. of Lacy MacAuley, at 2; Decl. of Legba Carrefour, at 2. Some of the disclosed posts would include the pictures and/or names of additional specific individuals who participated in particular political events, contain a list of intended attendees at specific political events, reflect Intervenors' involvement or affiliation with specific political organizations or groups, or propose or reveal political or organizational strategies unconnected to any alleged "riot" in the District of Columbia on January 20. *See* Decl. of Lacy MacAuley, at 2; Decl. of Legba Carrefour, at 2. The identities of thousands of Facebook users who

"liked" the disruptj20 Facebook page, and non-public lists of intended attendees at events associated with the disruptj20 page — including events, such as a peaceful dance-party protest to call attention to the anti-LGBTQ stance of the incoming Vice President, that are in no way associated with any alleged "riot" on January 20 — would be revealed to the government as well. *See* Decl. of Emmelia Talarico, at 1-2.

The warrants initially prohibited Facebook from disclosing their existence; after Facebook challenged the gag order, lost, and appealed, the government agreed on September 14, 2017, to permit disclosure of the warrants.

Facebook promptly notified the Intervenors that their accounts were the subject of search warrants. The Intervenors now seek relief from this Court to prevent the unjustified wholesale disclosure of three months' worth of personal and associational/expressive information pursuant to overbroad warrants. Facebook does not object to this motion. Counsel has asked the government for its position and the government has not responded.

ARGUMENT

Although the government ostensibly seeks to "seize" only information related to particular activities that are the subject of its criminal investigation, the warrants require Facebook to "disclose" far more: the entire contents of each Intervenor's account for a period of more than 90 days. No aspect of the warrants prohibits government investigators from accessing, examining, copying, and retaining all of the disclosed materials, to any extent it sees fit, on their way to "seizing" the material that is the target of the warrants — regardless of the connection, or lack thereof, between much of the "disclosed" materials and the object of the warrants.

The material that will be "disclosed" in this manner, despite its irrelevance to the government's investigation, is extensive. The warrants' broad sweep would enable the government

to review the targeted account owners' — and in many instances third parties' — intimate communications with romantic partners; names and family photographs of minor children; private communications on sensitive topics like domestic violence, prescription drugs, and psychiatric treatment; political and social affiliations and affiliations; choices to associate (i.e., become "friends" with on Facebook) or not associate with particular individuals, and views on a plethora of political, social, religious, and personal issues. The political activities, views, and associations of users and of identifiable third parties would also be revealed, as would specific proposals for political strategies and tactics having no relation to any alleged "riot" on Inauguration Day.

Because of the absence of safeguards, all of this information would be searched and then could be kept, copied, shared, and scrutinized with the same degree of investigative interest as the material the warrants authorize the government to "seize" formally. The warrants therefore authorize a seizure that is overbroad and unreasonable.

I. The Warrants Are Overbroad And Therefore Fail The Fourth Amendment's Particularity Requirement And Are Unreasonable.

Particularly in light of the First Amendment implications of rummaging through a mass of records of a person's speech and associational activities for three months, the government's extraordinarily broad disclosure demand fails the Fourth Amendment's requirement that search warrants must "particularly describ[e] the . . . things to be seized." U.S. Const. amend IV. Additionally, "the ultimate touchstone of the Fourth Amendment is reasonableness," *Riley v. California*, 134 S. Ct. 2473, 2482 (2014) (citation and internal quotation marks omitted), and the same problems going to particularity doom the warrants under that standard as well.

A. The Fourth Amendment prohibits "exploratory rummaging" by the government in a person's digital information, particularly when First Amendment-protected political and associational material is implicated.

The principal evil against which the Fourth Amendment was directed was the British practice of issuing "general warrants," which "allowed royal officials to search and seize whatever and whomever they pleased while investigating crimes or affronts to the Crown." *Ashcroft v. al-Kidd*, 563 U.S. 731, 742 (2011). Such warrants thereby "placed 'the liberty of every man in the hands of every petty officer.'" *Stanford v. Texas*, 379 U.S. 476, 481 (1965). "The manifest purpose of th[e] particularity requirement was to prevent general searches." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). "The problem posed by the general warrant is not that of intrusion [p]er se, but of a general, *exploratory rummaging* in a person's belongings." *Andresen v. Maryland*, 427 U.S. 463, 479 (1976) (citation, internal quotation marks, and source's alteration marks omitted, and emphasis added); *accord Buckner v. United States*, 615 A.2d 1154, 1155 (D.C. 1992) ("The particularity requirement prohibits sweeping, exploratory searches[.]").

To guard against the issuance of general warrants, the Fourth Amendment requires warrants to "particularly describ[e] the place to be searched and the persons or things to be seized." U.S. Const. amend. IV. "By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Garrison*, 480 U.S. at 84. Thus, particularity requires not only that a warrant describe the specific place to be searched and items to be seized but that the specifications are not so expansive and overly broad as to render the scope of the search akin to that permitted by a general warrant.

The problem of a general "exploratory rummaging," *Andresen*, 427 U.S at 479, is intensified when the rummaging is into constitutionally protected information about a person's beliefs, associations, and political activity. Courts have long recognized the chilling effect that government scrutiny of individuals' political speech and associations can have on the exercise of First Amendment freedoms. For instance, in *NAACP v. Alabama*, 357 U.S. 449 (1958), a state court had issued a contempt judgment against the civil rights organization for refusing to release a list of its members. The Supreme Court unanimously reversed, explaining that "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs," and, conversely, "compelled disclosure of affiliation with groups engaged in advocacy may constitute [an] effective [] restraint on freedom of association" because of "the vital relationship between freedom to associate and privacy in one's associations." *Id.* at 462. Therefore, "state action which may have the effect of curtailing the freedom to associate is subject to the closest scrutiny." *Id.* at 460-61; *accord Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 546 (1963); *see also AFL-CIO v. FEC*, 333 F.3d 168, 170 (D.C. Cir. 2003) (striking down regulation requiring disclosure of investigatory files concerning political associations because of the "substantial First Amendment interests implicated in releasing political groups' strategic documents and other internal materials"); *FEC v. Machinists Non-Partisan Political League*, 655 F.2d 380, 388 (D.C. Cir. 1981) (recognizing that the "release of [political associational] information to the government carries with it a real potential for chilling the free exercise of political speech and association guarded by the first amendment").

First Amendment freedoms may be threatened just as seriously by searches that *expose* a person's political associations and beliefs as by a government demand targeting that information.

As the Supreme Court has explained, "associational rights are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference, and … these rights can be abridged even by government actions that do not directly restrict individuals' ability to associate freely." *Lyng v. Int'l Union*, 485 U.S. 360, 367 n.5 (1988) (citation and internal quotation marks omitted); *accord Gibson*, 372 U.S. at 544. Accordingly, although the Fourth Amendment standards themselves do not change when expressive and/or associational material is at issue, courts have recognized for more than fifty years that the Fourth Amendment standard must be applied with "the most scrupulous exactitude" when material about First Amendment activity is at issue. *Stanford*, 379 U.S. at 485; *accord Maryland v. Macon*, 472 U.S. 463, 468 (1985); *see also Marcus v. Search Warrants*, 367 U.S. 717, 729 (1961) ("The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression. For the serious hazard of suppression of innocent expression inhered in the discretion confided in the officers authorized to exercise the power.").

For instance, in *Stanford v. Texas*, a state court had issued a warrant authorizing the search of a home for "books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments concerning the Communist Party of Texas, and the operations of the Communist Party in Texas." 379 U.S. at 478-79. Police officers spent more than four hours in the house, and a large amount of written material was "hauled off to an investigator's office." *Id*. at 479-80. Although the search warrant in *Stanford* may have been particular enough in its description "to pass constitutional muster[] had the things been weapons, narcotics or cases of whiskey," *id*. at 486 (quotation marks omitted), the Supreme Court condemned it as an unconstitutional general warrant because "it was not any contraband of that kind which was ordered to be seized, but literary

material." *Id*. Reviewing the history of abuses that led to the adoption of the Fourth Amendment, the Court held that "[t]he indiscriminate sweep of that language [in the warrant] is constitutionally intolerable. To hold otherwise would be false to the terms of the Fourth Amendment, false to its meaning, and false to its history." *Id*.

Following *Stanford*, and in keeping with its differentiation between literary material and contraband, courts have applied the Fourth Amendment standard with special care when materials concerning speech and associations are the objects of the search or seizure at issue. *See, e.g., Roaden v. Kentucky*, 413 U.S. 496, 502 (1973) ("The seizure of instruments of a crime, such as a pistol or a knife, or contraband or stolen goods or objects dangerous in themselves, are to be distinguished from quantities of books and movie films when a court appraises the reasonableness of the seizure under Fourth or Fourteenth Amendment standards." (citation and internal quotation marks omitted)); *Voss v. Bergsgaard*, 774 F.2d 402, 404-05 (10th Cir. 1985) (condemning as overbroad search warrants authorizing seizure of anti-tax organizations' customer records as well as "books, literature and tapes advocating nonpayment of federal income taxes; publications of tax protestor organizations" and the like; the court noted that"[t]he warrants' overbreadth is made even more egregious by the fact that the search at issue implicated free speech and associational rights" concerning an organization that espouses "dissident" views).

Today, an ever-increasing fraction of society's information, including information concerning private matters and political activities, is stored in electronic form. *See, e.g.*, Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. 581, 589 (Jan. 2011) ("[P]ersonal online data can reveal virtually everything about an Internet user, from her political affiliation to her geographic location, medical history, sexual preference, or taste in music."); Dee Pridgen, *Consumer Privacy in the Digital Marketplace: Federal Initiatives*, 33-OCT Wyo. Law.

14, 15 (2010) ("In the world of social media, users freely offer up all kinds of personal information, but with the understanding (or misunderstanding) that the provider, such as Facebook, will keep their personal information within certain limits."). The applicable constitutional principles — a prohibition on general searches and special "exactitude" when it comes to material regarding the exercise of First Amendment rights — must therefore be applied in a meaningful way to searches of electronic information, lest the "right of the people to be secure … against unreasonable searches and seizures," U.S. Const. amend. IV, lose most of its force in the modern world.

B. Searches for electronic information raise special privacy concerns given the breadth and quantity of personal and expressive/associative material individuals can store electronically.

Electronic communications, like their paper counterparts, are subject to a reasonable expectation of privacy and are therefore protected by the Fourth Amendment. *See In re Grand Jury Subpoena*, 828 F.3d 1083, 1090 (9th Cir. 2016); *Vista Marketing, LLC v. Burkett*, 812 F.3d 954, 969 (11th Cir. 2016); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). The storage capacity of electronic devices and online accounts have provided grounds for the government to seek to search a greater quantity of information than ever before in pursuit of evidence. And the government no doubt appreciates the ease and speed with which enormous amounts of private information can be vacuumed into its offices electronically. However, these very same qualities of electronic devices and accounts — their enormous capacity and fast data-transfer capabilities — "create[] a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam) ("*CDT*").

Courts have recognized, moreover, that the organization of life in the digital age makes electronic communications — including through social media platforms like Facebook — inevitable. *Id.* at 1177 ("Electronic storage and transmission of data is no longer a peculiarity or a luxury of the very rich; it's a way of life."); *In re U.S.'s Application For A Search Warrant To Seize & Search Elec. Devices From Edward Cunnius*, 770 F. Supp. 2d 1138, 1144 (W.D. Wash. 2011) ("*Cunnius*") ("Because it is common practice for people to store innocent and deeply personal information on their personal computers, a digital search of [electronically stored information] will also frequently involve searching personal information relating to the subject of the search as well as third parties.").

Social media's speed, convenience, reach, and ubiquity make it an attractive platform for individuals to store and share written and visual content, to connect with friends and fellow activists, to organize political movements, and to communicate about the most personal details of their lives. As a result, opening and reading the contents of a person's social media are the 21st-century equivalent of reading every letter the person ever sent, listening to every phone call the person ever made, and viewing every photograph the person ever took. *See In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, 2013 WL 4647554, at *8 (D. Kan. Aug. 27, 2013) ("*Email/Skype*") (likening warrants for all contents of an email account to "a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it constitutes fruits, evidence or instrumentality of a crime"); *accord Matter of Search of Info. Associated with Fifteen Email Addresses Stored at Premises Owned, Maintained, Controlled or Operated by 1 & 1 Media, Inc.*, 2017 WL 3055518, at *4 n.5 (M.D. Ala. July 14, 2017) ("*Fifteen Email Addresses*"). The Fourth Amendment "would not allow such a warrant and should therefore

not permit a similarly overly broad warrant just because the information sought is in electronic form rather than on paper." *Email/Skype*, 2013 WL 4647554, at *8. Just as law enforcement practices have adapted by seeking out electronic information from social media accounts, judicial enforcement of the Fourth Amendment must also adapt by ensuring that privacy protections keep up with the new risks to privacy posed by broad social media searches.

Acknowledging that searches of electronic information require the identification of information of legitimate law enforcement interest from among vast stores of information, the D.C. Rules of Criminal Procedure (like their federal counterparts) recognize the usefulness and presumptive propriety of a two-stage process in which the government first seizes or copies electronically stored information and then conducts a subsequent review for the more narrow subset of information that is the object of the warrant. *See* D.C. Super. Ct. Crim. R. 41(e)(2); Fed. R. Crim. P. 41(e)(2)(B).

Although the procedure is widely used, many courts have rightly recognized the threat to privacy that arises when a warrant gives the government carte blanche to acquire the entire contents of an electronic device or digital account (such as email or social media) without limitations about how government agents will search through or how long they will retain the material that is neither the justification for, nor the object of, the warrant. *See In the Matter of the Search of www.disruptj20.org That Is Stored at Premises Owned, Maintained, Controlled, or Operated by Dreamhost*, 2017 WL 4169713, at *3 (D.C. Super. Ct. Sept. 15, 2017) (Morin, C.J.); *Fifteen Email Addresses*, 2017 WL 3055518, at *4; *Email/Skype*, 2013 WL 4647554, at *8; *In re Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis*, 21 F. Supp. 3d 1, 8-9 (D.D.C. 2013) ("*Aaron.Alexis*"); *In re Search Warrant*, 71 A.3d 1158, 1183 (Vt. 2012) ("*Vt. Search Warrant*"); *Cunnius*, 770 F. Supp. 2d at 1151; *see also CDT*, 621 F.3d at 1177 ("The

process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect."); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (McConnell, J.) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important.").

"When reviewing vast amounts of information, it is understood that the government will inevitably come across material that falls outside the scope of the warrant." *Dreamhost*, 2017 WL 4169713, at *2; *accord Andresen*, 427 U.S. at 482 n.11. "Indeed, 'over-seizing' is considered to be an 'inherent part of the electronic search process' and often times provides the government with 'access to a larger pool of data that it has no probable cause to collect.'" *Dreamhost*, 2017 WL 4169713, at *2 (quoting *Aaron.Alexis*, 21 F. Supp. 3d at 8). Nonetheless, "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Andresen*, 427 U.S. at 482 n.11.

Understanding the problem and the threat to privacy begins with the obvious fact that information that is "disclosed" to the government in the first stage of the "disclose-then-seize" warrant is, in reality, no less "seized" by the government and within its power to examine than the much narrower range of information that the government says it will formally "seize" at the second stage. As a practical matter, the government will comb through the "disclosed" material — i.e., the entire contents of the electronic device or electronic account — to find the material it wishes to "seize." Courts have accordingly recognized that the "disclosed" material *is* for constitutional purposes "seized" and therefore that the first stage of the process is equally subject to Fourth

Amendment limitations as the second. As the federal court here in D.C. has explained, "By distinguishing between the two categories, the government is admitting that it does not have probable cause for all of the data that Facebook would disclose; otherwise, it would be able to 'seize' everything that is given to it. Yet despite this attempted distinction — which has no apparent basis in the Fourth Amendment — even the material that is not within this second 'seizure' category will still be turned over to the government, and it will quite clearly be 'seized' within the meaning of that term under the Fourth Amendment." *Aaron.Alexis*, 21 F. Supp. 3d at 8-9; *accord Fifteen Email Addresses*, 2017 WL 3055518, at *3 ("[W]here [a service provider] is compelled to 'disclose' data, and where the Government intends to search through and keep all such disclosed data regardless of relevance, there can be no doubt that all data encompassed by the warrant is effectively seized."); *Cunnius*, 770 F. Supp. 2d at 1150 ("Once the Court authorizes the government to search all data, the government can, and will.").

Does the Fourth Amendment permit investigators to open and read every file that is disclosed? View every picture and video? Use what they find to create dossiers (or enlarge the dossiers they already have) on political critics of the current presidential administration, as the Intervenors here are? Warrants that contain no safeguards or search protocols open up all of these troubling possibilities, which would be unreasonable and which the Fourth Amendment's prohibition of general warrants is aimed at curtailing. *See CDT*, 621 F.3d at 1171 ("Since the government agents ultimately decide how much to actually take, [the availability of additional information] will create a powerful incentive for them to seize more rather than less: … Let's take everything back to the lab, have a good look around and see what we might stumble upon."); *accord Aaron.Alexis*, 21 F. Supp. 3d at 6-7; *Email/Skype*, 2013 WL 4647554, at *8-9; *Cunnius*, 770 F. Supp. 2d at 1151. As this Court has admonished, "The Warrant does not, and should not,

grant carte blanche access to those materials for which the government has not established probable cause." *Dreamhost*, 2017 WL 4169713, at *3.

Proceeding from the common-sense and constitutionally-mandated premise that both stages of a "disclose-then-seize" warrant constitute seizures and recognizing that, absent protocols to minimize invasions of privacy, this type of warrant effectively enables "exploratory rummaging," a number of courts have held invalid (or refused to issue) "disclose-then-seize" warrants that lack adequate procedural safeguards, *see Fifteen Email Addresses*, 2017 WL 3055518, at *4-5; *Email/Skype*, 2013 WL 4647554, at *8-9, *Cunnius*, 770 F. Supp. 2d at 1152-53, or (like this Court) have required safeguards to salvage "disclose-then-seize" warrants. *See Dreamhost*, 2017 WL 4169713, at *3-4; *Aaron.Alexis*, 21 F. Supp. 3d at 9-10. One court, in affirming the imposition of nine safeguards, *Vt. Search Warrant*, 71 A.3d at 1186, characterized these types of limits as "essential to meet the particularity requirement of the Fourth Amendment, especially in cases involving record searches where nonresponsive information is intermingled with relevant evidence," *id.* at 1184. Such safeguards may include "asking the electronic communications service provider to provide specific limited information such as emails containing certain key words or emails sent to/from certain recipients, appointing a special master with authority to hire an independent vendor to use computerized search techniques to review the information for relevance and privilege, or setting up a filter group or taint-team to review the information for relevance and privilege." *Email/Skype*, 2013 WL 4647554, at *10; *accord CDT*, 621 F.3d at 1179-80 (Kozinski, C.J., concurring); *Aaron.Alexis*, 21 F. Supp. 3d at 11; *Vt. Search Warrant*, 71 A.3d at 1162-63. Courts have also suggested or applied additional safeguards, such as requiring the government to waive reliance on the plain-view doctrine, *see CDT*, 621 F.3d at 1179-80 (Kozinski, C.J., concurring); *Aaron.Alexis*, 21 F. Supp. 3d at 11, or inserting steps in the

review process that enable the identification of appropriate minimization procedures with subsequent review by the court, *see Dreamhost*, 2017 WL 4169713, at *3-4.

Not all courts have imposed such safeguards. Often, however, the rationale for declining to apply such safeguards is that the material at issue is child pornography, which of course lacks any First Amendment protection, *see New York v. Ferber*, 458 U.S. 747 (1982), and which is often carefully hidden behind innocuous file names. *See United States v. Schesso*, 730 F.3d 1040, 1049-50 (9th Cir. 2013) (noting that child pornography offenders "go to great lengths to conceal and protect from discovery their collection of sexually explicit images of minors" and rejecting overbreadth challenge where the search at issue "did not involve an over-seizure of data that could expose sensitive information about other individuals not implicated in any criminal activity … nor did it expose sensitive information about Schesso other than his possession of and dealing in child pornography."). Such cases are of limited assistance where, as here, extensive political and associational material is implicated. Moreover, as compared with the opinions taking a laxer view toward Fourth Amendment protections, decisions that *have* recognized the threats to privacy posed by a two-step protocol with no safeguards — including the recent decision from this Court — are simply better reasoned and more faithful to the history of the Fourth Amendment and its overriding objective of prohibiting general warrants.

This case does not require the Court to decide whether the two-step process can never be constitutionally imposed without safeguards. Rather, in light of the extensive political, associational, and expressive content that — in spite of their irrelevance to the government's investigation — would be disclosed to government officials in this case, and the "scrupulous exactitude" with which Fourth Amendment strictures apply when First Amendment-protected material is at stake, the Court should at a minimum hold that where such material is at issue, the

Fourth Amendment *requires* procedural safeguards. Their absence in the warrants at issue exposes both deeply personal and expressive/associational material to unlimited government examination — and is therefore fatal to the constitutionality of the warrants both under the particularity inquiry and Fourth Amendment reasonableness generally.

C. By exposing extensive private and First Amendment-related information without any safeguards, the warrants at issue authorize "exploratory rummaging" in the nature of a general warrant and therefore are invalid.

The warrants at issue leave no pixel unturned in describing what must be disclosed. They require Facebook to reveal all of Lacy MacAuley's and Legba Carrafour's personal messages, chats, photos and videos, wall postings, searches, and status updates. The required disclosures also include a list of groups that these users have joined, their Facebook "friends," the searches they have performed, and their pending and rejected "friend" requests. In other words, the warrants require Facebook to turn over a complete record of the account owners' private communicative activity and individual and group associations on Facebook for the specified period.

The declarations of the individual Intervenors here confirm that the types of information contained in these wholesale disclosures would paint a detailed picture both of intimate aspects of the Intervenors' lives and of their political and associational activities. *See* Decls. of Emmelia Talarico, Lacy MacAuley, and Legba Carrefour (attached as Exhibits B, C, and D, respectively). The disclosed materials, including an individual's medical and psychiatric information, credit card and password information, personal photographs of family members including children, romantic messages and discussions of the domestic violence that an Intervenor or third parties have suffered, would reveal personal information that the government has no business perusing. And the political and associational material implicated — what political events the Intervenors organized and attended, who else was there, what they hoped to accomplish, and their political beliefs and

associational affiliations themselves — would make government agents privy to posts discussing and debating political opinions, proposing organizing strategies, or identifying individuals associated with certain groups and causes, including groups and causes antithetical to the current Administration on whose behalf the investigating agents are acting. Such disclosures would obviously chill protected speech and associational activities, particularly activities associated with dissenting viewpoints.

Additionally, the warrant for the disruptj20 Facebook page would reveal who planned to attend certain events (including a peaceful dance party aimed at calling out the anti-LGBTQ views of the incoming Vice President) that had nothing to do with any "riot" on January 20, as well as the thousands of individuals who "liked" the disruptj20 page — an act that is of course no crime but rather a pristine exercise of First Amendment rights of expression and association. *See, e.g.*, *Elfbrandt v. Russell*, 384 U.S. 11, 19 (1966) ("A law which applies to membership without the 'specific intent' to further the illegal aims of the organization infringes unnecessarily on protected freedoms."); *Bland v. Roberts*, 730 F.3d 368, 385-86 (4th Cir. 2013) (holding that "liking" on Facebook constitutes protected speech). Indeed, "liking" a Facebook page does not even indicate that one agrees with the contents of the page; it may be no more than a means of signing up to receive posts from the page in a Facebook newsfeed, akin to subscribing to a magazine or getting on a particular organization's email list. Still, the consequences of being tagged in a government investigation as associated with a political page that the government views as related to criminal activity may be enough to deter casual "likers" of controversial or dissident political pages in the future. The government's seizure of a list of the disruptj20 page "likers" thus would chill both serious supporters and curious visitors alike. *Cf. Stanley v. Georgia*, 394 U.S. 557, 564 (1969) (recognizing that "the Constitution protects the right to receive information and ideas").

All of this information, it bears repeating, is wholly apart from the subject matter that is the government's justification for seeking the warrants and the information that the warrants ostensibly target: information concerning specific allegations of "rioting" at a particular time and place. Search Warrants, Attachment B, at 4. In sum, on their way to finding the information relevant to its investigation (even assuming there is any), the government will have both access to, and an unlimited opportunity to scrutinize, numerous irrelevant but private communications involving First Amendment-protected political and associational activity, as well as some of the most personal aspects of Intervenors' lives and the lives of third parties. The mere recitation of the scope of the intrusions that the warrants would authorize is enough to demonstrate that they are unreasonable in relation to the government's objective.

Even more than the warrant in *Stanford*, the warrants here are, in reality, general warrants. The contents of a Facebook account may easily contain more personal and political information than was seized in that case. Indeed, "a single gigabyte of storage space is the equivalent of 500,000 double-spaced pages of text." *Cunnius*, 770 F. Supp. 2d at 1144. The warrants here, seeking all communicative content from three Facebook accounts for more than 90 days, are an order of magnitude less particularized than the warrant in *Stanford*. Rather than spending four hours in the users' homes deciding what to seize, government agents here propose to seize what amounts to *all* the papers in the users' homes, and then spend four, forty, or four hundred hours sifting through them looking for evidence. As in *Stanford*, "[t]he indiscriminate sweep of [the] language [in the warrant] is constitutionally intolerable." 379 U.S. at 486.

That the words and pictures sought here are in electronic form and have been transmitted on the internet is of no help to the government because First Amendment protections are no less robust on the internet. *See Reno v. ACLU*, 521 U.S. 844, 870 (1997); *Solers, Inc. v. Doe*, 977 A.2d

941, 950 (D.C. 2009) "While in the past there may have been difficulty in identifying the most important places. . . for the exchange of views, today the answer is clear. It is cyberspace — the vast democratic forums of the Internet in general, and social media in particular." *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017) (quotation marks and citation omitted).

Nor does the fact that the words and pictures sought here are in electronic form make it impossible for the government to satisfy the particularity requirement of the Fourth Amendment in the manner required in cases involving First Amendment material. For example, the warrants could have authorized a search limited by certain keywords, or for communications on certain topics or with particular individuals. *See Aaron.Alexis*, 21 F. Supp. 3d at 11 ("[T]he premise … that law enforcement ha[s] to open every file and folder to search effectively[] may simply no longer be true.); *Vt. Search Warrant*, 71 A.3d at 1182-85 (affirming imposition of search condition requiring the use of targeted searches based on dates, key words, and file types). The Eleventh Circuit recently opined in a prostitution case that "disclose-then-seize" warrants to Facebook sought "disclosure to the government of virtually every kind of data that could be found in a social media account … unnecessarily"; instead, the warrants could have been limited, for instance, to messages by particular persons suspected of being prostitutes or customers, and such a search would have been both "targeted" and "not … impractical" for Facebook. *United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017). Although the court did not decide whether the warrants violated the Fourth Amendment because the good-faith exception applied, the court strongly disagreed with the suggestion that the government could not tailor the warrants. And nothing prevents the government from seeking a second set of broader warrants if probable cause to do so emerges from its initial and more carefully tailored search. *See Fifteen Email Addresses*, 2017 WL 3055518, at *5; *Vt. Search Warrant*, 71 A.3d at 1184-85.

If the government had made a persuasive showing that these options were insufficient for its legitimate needs, it could have incorporated a more detailed search protocol or any of a number of procedural safeguards that courts have suggested in grappling with the Fourth Amendment's application to digital searches. *See supra* Part I.B. As issued, however, the warrants would allow government investigators to examine the speech of myriad Facebook users in the course of sweeping up all communications with the Intervenors' accounts over a three-month period, including communications with family members, with romantic partners, and with political allies. And by uncovering the identities of everyone who has "liked" the disruptj20 Facebook page, the government will have learned something about the political predilections of approximately 6,000 people. *See* Decl. of Emmelia Talarico, at 2.

In today's world, a Facebook account is at once a message board, an email service, a diary, a calendar, a photo book, a video archive, and much more. It encompasses everything from an individual's public posts and private messages to her "check ins" at locations and records of what she has "liked," become a "fan" of, or searched for. *See Aaron.Alexis*, 21 F. Supp. at 3-4. As a repository of private information, a Facebook account is akin to a private home for Fourth Amendment purposes. *See, e.g.*, *United States v. Galpin*, 720 F.3d 436, 446-47 (2d Cir. 2013) (holding that a hard drive is like a residence for Fourth Amendment purposes); *United States v. Riccardi*, 405 F.3d 852, 861-63 (10th Cir. 2005) (same); *cf. Riley*, 134 S. Ct. at 2491 ("[A] cell phone search would typically expose to the government far more than the most exhaustive search of a house[.]"); *Grand Jury Subpoena*, 828 F.3d at 1090 ("Personal email can, and often does, contain all the information once found in the 'papers and effects' mentioned explicitly in the Fourth Amendment."). Examining the entirety of a person's Facebook account is therefore not a particularized search but a classically overbroad fishing expedition or "exploratory rummaging."

Four hours in the target's home was too much for the Constitution to tolerate in *Stanford*. The warrants at issue here would put government agents metaphorically, but realistically, hovering behind the Intervenors' shoulders in their homes, their offices, and even their bedrooms for more than *90 days* as they use Facebook on their computers or phones. That result is incompatible with the Fourth Amendment, particularly in light of the "scrupulous exactitude" with which its commands must be applied when First Amendment rights are at stake. The Court should accordingly quash the warrants, without prejudice to their reissuance with appropriate safeguards that protect the target account owners' privacy by minimizing intrusions into irrelevant private information. *See Dreamhost*, 2017 WL 4169713, at *3 (rejecting "carte blanche access to those materials for which the government has not established probable cause.").

II. In The Alternative, The Court Should Limit The Warrants By Appointing a Special Master As A Safeguard Between The Intervenors' Un-Seizable Information And The Prosecutors.

Even if the Court finds that safeguards are not required by the Fourth Amendment, the privacy and expressive/associational concerns that Intervenors raise justify, at a minimum, this Court's exercise of its discretion to impose procedural safeguards. In the *Dreamhost* case, which presented similar threats to constitutional values of privacy and association, the Court required such safeguards. *See Dreamhost*, 2017 WL 4169713, at *3 ("[B]ecause potential evidence is co-mingled with other information, the Warrant in its execution will implicate the privacy and First Amendment rights of website operators and innocent parties who visited or exchanged with the site and engaged in lawful associational and information gathering activity."). Courts around the country have recognized their authority to impose such conditions. *See Aaron.Alexis*, 21 F. Supp. 3d at 2, 9; *Vt. Search Warrant*, 71 A.3d at 1186; *Cunnius*, 770 F. Supp. 2d at 1150; *see also In the Matter of the Application of the United States of Am. for an Order Relating to Telephones Used*

by [Suppressed], 2015 WL 6871289, at *4 (N.D. Ill. Nov. 9, 2015) (imposing minimization requirements on search of cell phone location information). As this Court explained, "additional safeguards on electronic search warrants may be reasonable and appropriate to limit the possibility of abuse by the government." *Dreamhost*, 2017 WL 4169713, at *2; *accord CDT*, 621 F.3d at 1178-80 (Kozinski, C.J., concurring).

Of the various safeguards that might be imposed, the engagement of a special master to review and identify information that the government is authorized to seize under the warrants is the most advisable. *See Vt. Search Warrant*, 71 A.3d at 1182 (affirming imposition of search warrant conditions and upholding conclusion that "resorting to a neutral third-party screener may be the only way to provide meaningful privacy protections in the face of broad law enforcement requests"); *CDT*, 621 F.3d at 1180 (Kozinski, C.J., concurring) (recommending that "[s]egregation and redaction of electronic data must be done either by specialized personnel or an independent third party"). A special master appointed by the Court would be neutral. A special master would have no ancillary investigative incentive to linger over private material but instead could proceed directly and most efficiently to the identification of relevant material. A special master would obviate any concern on the part of the government that it could incur *Brady* obligations by coming into possession of material that is not the target of the warrants but which could nonetheless be material and exculpatory. A special master would not require any of the easily-breached logistical and organizational measures within the U.S. Attorney's Office that would be necessary if the identification of responsive material from the target Facebook accounts were conducted by a "privilege team" or "taint team" consisting of government personnel. *See, e.g., In re Grand Jury Subpoenas*, 454 F.3d 511, 523, 524 (6th Cir. 2006) (reversing appointment of taint team and requiring appointment of special master to review subpoenaed documents for privilege, and noting

that "taint teams present inevitable, and reasonably foreseeable, risks to privilege, for they have been implicated in the past in leaks of confidential information to prosecutors" and have "a conflicting interest in pursuing the investigation"); *United States v. Stewart*, 2002 WL 1300059, at *6, *10 (S.D.N.Y. June 11, 2002) (appointing special master rather than privilege team to review seized material for privilege and warrant compliance, and noting that "at least three courts that have allowed for review by a government privilege team have opined, in retrospect, that the use of other methods of review would have been better"); *see also* John Simerman, *With Danziger Bridge pleas, federal judge unloads on top government officials*, New Orleans Advocate, Apr. 24, 2016 (reporting on fallout from leaks by leader of government "taint team" in high-profile prosecution).

The fact that a special master would not be a government prosecutor or investigator is a strength of this safeguard, not a weakness. As the Supreme Court has observed, when it comes to the Fourth Amendment, the difference between "a neutral and detached magistrate" and "the officer engaged in the often competitive enterprise of ferreting out crime" is one of significant constitutional magnitude. *Johnson v. United States*, 333 U.S. 10, 14 (1948). The master would not be distracted by the urge to veer from the contours of the warrants by following hunches arising from irrelevant material or by investigating evidence in "plain view" among information that law enforcement did not have probable cause to search in the first place. *See CDT*, 621 F.3d at 1171 (noting that permitting use of plain view evidence in the electronic context "create[s] a powerful incentive for [the government] to seize more rather than less"). To the extent that the government could fear that the special master would not be sufficiently familiar with the government's investigation to understand what materials would be responsive, the government can provide any instructions or training materials it wishes for the purpose of enhancing the master's understanding. *See Vt. Search Warrant*, 71 A.3d at 1182. Indeed, outside of the electronic context,

the government has this same opportunity to influence the scope of the warrants — by making a showing to a neutral officer (in that case, a judge or magistrate) explaining what the investigation concerns and what information would therefore be relevant.

If this Court declines to quash the warrants outright and orders safeguards instead, this Court might, in light of its experience adjudicating *Dreamhost* and the government's repeated attempts through the proposed-order process there to reach beyond the parameters set by this Court's prior orders, find it most expedient to order review by a special master directly.

III. The Court Should Carefully Scrutinize The Question Of Probable Cause.

Because Intervenors do not currently have access to the sealed affidavit on which the search warrant was based, they cannot argue with specificity that probable cause to seize all of the identified categories of materials from their accounts was lacking. However, Intervenors are aware that in the *Dreamhost* matter, counsel for third-party "John Doe" individuals whose First Amendment interests were implicated by the search warrant there found numerous ambiguities and misleading aspects of the affidavit that might not have been apparent to the judge who reviewed the warrant ex parte.

Given the relatedness of that case to this one, Intervenors urge the Court to give careful consideration to the question whether the warrants at issue here suffer from deficiencies of probable cause in addition to particularity. The Court might consider ordering the warrant application unsealed (in full or in redacted form) so that it could benefit from adversary presentation on this issue. In any event, Intervenors reserve the right to make a more specific showing regarding probable cause when the necessary material becomes available.

CONCLUSION

For the foregoing reasons, the Court should quash the warrants, granting leave to the government to seek new warrants that meet Fourth Amendment standards. In the alternative, the Court should appoint a special master who is authorized to identify the information that the government is entitled to *seize* (listed in Search Warrants, Attachment B, Part II), and convey to the government only that material and no more.

Respectfully submitted,

September 28, 2017

Scott Michelman (D.C. Bar No. 1006945)
Arthur B. Spitzer (D.C. Bar No. 235960)
Shana Knizhnik (D.C. Bar No. 1020840)
American Civil Liberties Union Foundation
of the District of Columbia
4301 Connecticut Avenue, N.W., Suite 434
Washington, D.C. 20008
(202) 457-0800
smichelman@acludc.org

Counsel for Intervenors

CERTIFICATE OF SERVICE

I hereby certify that, on this 28th day of September 2017, I caused copies of the foregoing MOTION OF INTERVENORS TO QUASH OR NARROW SEARCH WARRANTS along with its accompanying exhibits and a proposed order, to be served on counsel for the Government and counsel for Facebook by first-class mail, postage prepaid, as well as by email, as follows:

John Roche
Perkins Coie LLP
700 Thirteenth Street, N.W. Suite 600
Washington, DC 20005-3960
JRoche@perkinscoie.com

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

Scott Michelman (D.C. Bar No. 1006945)
American Civil Liberties Union Foundation
of the District of Columbia
4301 Connecticut Avenue, N.W., Suite 434
Washington, D.C. 20008
(202) 457-0800
smichelman@acludc.org

Counsel for Intervenors