VIRGINIA:

IN THE CIRCUIT COURT OF LOUNDOUN COUNTY

IN RE: SEARCH WARRANTS FOR INFORMATION ASSOCIATED WITH FACEBOOK ACCOUNT FREETHEMALLVA, STORED AT PREMISES CONTROLLED BY FACEBOOK, INC.	)))))	Misc. Case No. _____

MOTION OF INTERVENORS MADHVI VENKATRAMAN, DOE 1, DOE 2 AND DOE 3 TO QUASH OR NARROW SEARCH WARRANT

TABLE OF AUTHORITIES

CASES

CONSTITUTION, STATUTES AND RULES

MISCELLANEOUS

Introduction

Intervenors, four individuals associated with a local political advocacy group, hereby move to quash or narrow a search warrant that would force Facebook to disclose to the Leesburg Police Department the contents of a Facebook account that advocates the release of individuals held in migrant detention, jails, and prisons in the State of Virginia, contrary to the position held by many elected officials. The warrant is manifestly overbroad. Most of the material demanded bears no relation to the investigation for which the police sought the warrant.

Permitting government officials to comb through messages about political activity and associations, and to identify nearly more than a hundred anonymous Facebook users who have chosen to associate with the page, is an unjustified invasion of privacy harkening back to the "general warrants" that the Fourth Amendment was enacted to prohibit. Additionally, the enforcement of the warrant would chill future online communications of political activists and people who follow or communicate with them, by showing that no Facebook privacy setting can protect against government snooping into political materials far removed from any proper law enforcement interest.

Intervenors recognize the need to sort relevant from irrelevant information in the context of an electronic search. The warrant here, however, contains safeguards or minimization procedures, and thus allow the government to peruse the Intervenors' content at whatever level of detail and using whatever search tools they wish. Particularly where, as here, First Amendment concerns regarding political association are implicated, the absence of procedural safeguards renders the warrants fatally defective under the First and Fourth Amendments. The Court should quash the warrant or, at the very least, impose procedural safeguards adequate to protect the fundamental associational and privacy interests at stake.

STATEMENT OF THE CASE

In July 2020, a group of area residents, including intervenor Madhvi Venkatraman, who were alarmed by unhealthy conditions faced by Virginians suffering from unnecessary detention, formed a political advocacy group called Free Them All VA. Their group is a coalition of organizations and individuals that oppose mass incarceration and endeavors to aid the organizing efforts of individuals incarcerated in Virginia detention centers, jails, and prisons. The group created a Facebook page to disseminate information about the conditions in Virginia detention centers and to amplify the demands and concerns of people who have been detained. The Facebook page also serves as a way for directly affected people to get into contact with the coalition. The page, named FreeThemAllVA, is located at www.facebook.com/FreeThemAllVA. Venkatraman is the owner of the page and, as of September 2020, she was one of three administrators ("admin") of the page. Ventkatraman Affidavit ¶¶ 2-5; Doe 1 and Doe 2 are "editors" of the page. Doe 1 Affidavit ¶ 3; Doe 2 Affidavit ¶ 3.

On the evening of September 11, 2020, some members of Free Them All VA participated in a political demonstration outside the home of Virginia Attorney General Mark Herring, calling for him to end the detention of immigrants at a facility in Farmville, which is the site of the largest outbreaks of COVID-19 at any immigrant detention center in the United States. According to press reports, demonstrators painted a political slogan, "Free Them All," in both Spanish and English on the sidewalk outside the Herring residence. *Protesters Leave Graffiti Outside AG's Home*, Loudoun Now, Sept. 14, 2020, available at https://loudounnow.com/2020/09/14/protesters-leave-graffiti-outside-ags-home/. The demonstration was livestreamed on the FreeThemAllVA Facebook page. Levy Affidavit Exhibit A.

On September 15, 2020, a police officer with the Leesburg police department, Detective John Mocello, executed an affidavit seeking issuance of a search warrant directed at Facebook for the purpose of investigating the crime of destroying property. The officer averred that members of the group had painted lettering on the sidewalk; that the paint had to be removed professionally at a cost of under $1000; and that videos and pictures "of this destruction and of those involved in committing the destruction" had appeared on the Facebook page for a period of time but had been removed from public view.

Although the search warrant was sought to "assist in potentially determining who is responsible for this offense," *id.*, a far more sweeping warrant was requested. The warrant requires production of "Any and all subscriber records including subscriber name, address, phone numbers, length of service, credit card information, email address(es), and recent login/logout IP address(es)" as well as "Any and all wall content/posts, messages, chats, videos, and pictures to included [sic] deleted material," for the period between midnight on September 10, 2020 "through the present." Levy Affidavit Exhibit B.

Thus, the data covered by the warrant extends far beyond the videos and photos cited in the warrant affidavit as the basis for the search. Members of the public, including the families of those detained, have sent messages to the Free Them All VA coalition about the problems affecting individuals in detention, identifying detained individuals by name and criticizing corrections and law enforcement officials by name. Because many of those in detention are undocumented immigrants, they could be subject to retaliation by agents of Immigrations and Custom Enforcement ("ICE") if they are identified as having been the subject of discussion with the Free Them All VA coalition; it is also possible that the friends or family members who sent messages to the coalition could be

subject to retaliation. Doe 1 Affidavit ¶ 9. Several individuals, including Ventkatraman and Doc 1 and Doe 2, have functioned as "admins" or "editors" for the page, allowing them to post and amend content; but only movant Venkatraman has made her name public in connection with the coalition. Ventkatraman Affidavit ¶ 5; Doe 1 Affidavit ¶ 3; Doe 2 Affidavit ¶ 3. The other administrators and editors, including Intervenors Doe 1 and Doe 2, are subject to losing their anonymity if the search warrant is enforced. Still other members of the public have posted comments to the page; they, too, could be subject to having their identities disclosed pursuant to the warrant

As of today, 56 members of the public have "liked" the FreeThemAllVA page (including Doe 3, Doe 3 Affidavit ¶ 4), and 112 people have "followed" the page (the numbers were slightly lower last month). All of these people are currently anonymous. When a Facebook user "follows" a page, she receives (subject to Facebook's algorithms) notices in her newsfeed whenever new material is posted to the page being followed. It is comparable to a subscription to the page being followed. When a Facebook user "likes" a page, it is an indication of support for the page—comparable to stating that the user is a fan of that page. Venkatraman ¶ 10. The "like" is visible to the user's own network of Facebook friends; those likes are sometimes promoted to the user's friends, encouraging them to like or follow the page as well. By default, when a Facebook user likes a page, she becomes a "follower" of the page. See *What does it mean when someone likes or follows a Page?*, https://www.facebook.com/help/ 171378103323792. For the most part, the identities of Facebook users who "like" and who "follow" a page cannot be discerned from the page itself (although the Facebook friends of someone who "likes" a page may be able to see that the page is among that friend's "likes"). Otherwise, likers and followers are anonymous to the general public, unless Facebook is compelled to reveal those identities pursuant to a search warrant such as the warrant in

this case.

None of these people have made their names public, but as written, the warrant could be understood as commanding Facebook to produce detailed identifying information about all of them, potentially putting both them, their clients, and their families at risk. Doe 1 Affidavit ¶ 12; Doe 2 Affidavit ¶¶ 6, 7. And the prospect of being identified as being associated with the page will undoubtedly having a chilling effect, discouraging other members of the public from participating in the page's speech, from expressing support among their own friends for the page, and from sending message to the Free Them All VA coalition about issues of public concern. Ventrakamaan Affidavit ¶ 11; Doe 1 Affidavit ¶ 10; Doe 2 Affidavit ¶ 9.

The affidavit was served on Facebook, which, pursuant to its standard practices notified Madhvi Venkatraman that the warrant had been served. Levy Affidavit Exhibit C. Facebook gave her until October 12, later extended to October 13 because October 12 was a legal holiday, to file a motion to quash before any data would be released. Levy Affidavit ¶ 7 and Exhibit C. Under standard procedures, the data covered by the warrant would have been preserved pending resolution of any motion to quash. Levy Affidavit ¶ 9.

Accordingly, Venkatraman, along with some of the anonymous users of the page who are worried about losing their right to engage in anonymous speech or association, now move to quash the search warrant to the extent that it is overbroad.

ARGUMENT

Although the Commonwealth purportedly seeks only a video and photos that might reveal the identities of specific individuals who painted slogans on a Leesburg sidewalk, the warrant requires Facebook to disclose the entire contents of the FreeThemAllVA Facebook page for a period

of six days or more. 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, 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 warrant's broad sweep would enable the government to review private communications on issues of public concern, including discussions of strategy about how to express disagreement with elected officials and build public opposition to their policies and practices, as well as to identify individual detained individuals and their families who could easily be targeted for discrimination or retaliation in circumstances in which they are exceptionally vulnerable. The warrant would enable the reviewing law enforcement officials to identify many individuals who have chosen to participate in the Free Them All VA coalition, or to associate with its Facebook page, while remaining anonymous to protect against the danger that their employers, families or neighbors might express unhappiness about their activities and subject them to economic or other forms of retaliation. 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 destruction of property through painting a slogan on a Leesburg sidewalk.

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 that the search warrant affidavit identified as being the true target of the search: the video and photos of the September 11 demonstration. The warrants therefore authorize a seizure that is

overbroad and unreasonable.

I. The Warrant Is Overbroad, Fails the Fourth Amendment's Particularity Requirement, and Is Unreasonable.

Particularly in light of the First Amendment implications of rummaging through a mass of records of political group's speech and associational activities, the police department'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*, 573 U.S. 373, 381 (2014) (citation and internal quotation marks omitted), and the same problems of particularity doom the warrant under that standard as well.

A. The search warrant fails the Fourth Amendment's particularity requirement.

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).

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. (emphasis added). "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. So, for example, a warrant for the search of a personal computer fails the particularity requirement of the Fourth Amendment if, in addition to describing computer records as the items to be searched, it fails to limit the evidence to be seized to specific computer records that could be evidence of the crime that justified issuance of the warrant. *United States v. Cobb*, 970 F.3d 319, 328 (4th Cir. 2020).

The search warrant in this case fails Fourth Amendment standards for this reason alone. Although the probable cause affidavit makes clear that only the deleted video and pictures would be evidence of the alleged crime, the warrant calls for seizure of the entire contents of the Facebook page over a period of at least six days (September 10 through September 15). Indeed, because private messages sent before September 10 remained accessible to administrators and editors of the page during the period covered by the search warrant, it is quite possible that two months' worth of private messages stand to be forcibly disclosed if the search warrant is enforced. Venkatraman Affidavit ¶ 9. Facebook has not responded to questions about its understanding of the scope of the search warrant. Levy Affidavit ¶ 5.

B. The Fourth Amendment prohibition of "exploratory rummaging' by the government in a person's digital information is enhanced when First Amendment-protected political and associational material is implicated.

The problem of a general "exploratory rummaging," *Andresen*, 427 U.S at 479, is intensified when the information at issue is constitutionally protected speech or other data 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 (internal 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.

C. 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 Commonwealth 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*, 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 a person ever sent, listening to every phone call a person ever made, and viewing every photograph a 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"). 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. In acknowledgment of the fact that searches of electronic information require the identification of

information of legitimate law enforcement interest from among vast stores of information, the Federal Rules of Criminal Procedure now 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 Fed. R. Crim. P. 41(e)(2)(B).

Other courts have also 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.); *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. at482 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 particularity limitations as the second. As one federal court 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; *Cunnius*, 770 F. Supp. 2d

at 1150 ("Once the Court authorizes the government to search all data, the government can, and will.").

As another 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. Warrants that contain no safeguards or search protocols opens up the troubling possibility that investigators will read every file, view every photo, even use the information collected to build dossiers on political critics. *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. Such practices verge on the intrusive practices that the Fourth Amendment's prohibition of general warrants is aimed at curtailing.

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 Email/Skype*, 2013 WL 4647554, at *8-9; *Cunnius*, 770 F. Supp. 2d at 1152-53, or 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. Requiring the government to proceed by way of keyword search protocols is, in most cases, "necessary to prevent the warrants from becoming 'the internet-era version of a general warrant'", *U.S. v. Matter of Search of Info. Associated with Fifteen Email Addresses Stored at Premises Owned , Maintained, Controlled or Operated by 1&1 Media,* 2017 WL 8751915, at *2 (M.D. Ala. Dec. 1, 2017), *quoting United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017), 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; *In re Search of Information Associated with Facebook Accounts DisruptJ20, Lacymacauley, and Legba.Carrefour that is Stored at Premises Controlled by Facebook*, 2017 WL 5502809 (D.C. Super Ct. Nov. 9, 2017) (Morin, Ch. J.) ("*DisruptJ20*").

D. If the warrant is not quashed as overbroad, the Court should require the use of a three-step process to minimize impact on protected free speech.

In *DisruptJ20*, the Chief Judge of the Superior Court for the District of Columbia addressed this problem in considering search warrants served on Facebook in the course of investigating riots that occurred in Washington following protests over the inauguration of President Donald Trump on January 20, 2017. 2017 WL 5502809 (D.C. Super Ct. Nov. 9, 2017). Chief Judge Morin required the government to follow a three-step process to determine which data from a Facebook political action page could be turned over to the government for use in its criminal investigation. *Id.* at *13-*14. Facebook set aside the computer records from the Facebook page of a group called DisruptJ20, and from the Facebook accounts of two DisruptJ20 members who were suspected of organizing and planning riot activities separate from the peaceful protests involving civil disobedience that had been overtly advocated on the DisruptJ20 page. The government was not, however, permitted to examine those computer records manually. The first step in the review process was for the government to develop an electronic search protocol that would provide its exclusive means of accessing the electronic database that Facebook was to set aside, and the sole method for ascertaining which specific records it wanted to review manually. The search protocol had to be submitted to the court for its review. The second step, once the court had approved the search protocol, allowed the government to apply the search protocol to the database, but at that point the government was to provide a listing to the Court specifying which specific records the government wanted to be allowed to examine manually, and why the search protocol justified that examination. The court would then decide whether the government could seize them. Only at that point, under Chief Judge Morin's ruling, could the third step occur: the government could then

"seize" the records that the Court has determined were pertinent, and could read their contents. In addition, the court also imposed strict limits on the government's use of the records: data not found through this process to be evidence of a crime was to be deleted from the records, and not to be shared with any other government agency. *Id.* at *13, *14, *20.

In this case, Intervenors have indicated that the FreeThemAllVA Facebook page was not used in organizing the demonstration, and that private messages to the page did not relate to the demonstration (and, thus, to the crime that was allegedly committed during the demonstration). The Commonwealth need not, of course, take Intervenors' word on this. But by compelling the use of a court-approved search protocol for reviewing the electronic data, rather than allowing the police to conduct a front-to-back review that would give law enforcement officials the ability to read political and personal communications aimed at constraining their actions through means of lawful protest, not to speak of sensitive personal details about detained migrants and their families, the Court can protect the freedom of political association while ensuring that legitimate law-enforcement objectives are met. By adopting Chief Judge Morin's technique, the Court can avoid giving law enforcement officials access, via "exploratory rummaging," to private details such as the worries of immigrant families about the plight of named detained love ones, or disclosure of sensitive details about health or immigration status in the course of asking for help addressing these concerns, and it can avoid the chilling effect that enforcing the search warrant as written would certainly have.

This case does not require the Court to decide whether the normal two-step process for search warrants directed to electronic records can ever be constitutionally imposed without safeguards. Rather, in light of the extensive political, associational, and expressive content that—in spite of their irrelevance to the police investigation—would be disclosed to the Leesburg police 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 comparable to those imposed by Chief Judge Morin in *Disrupt J20* . Their absence in the warrants at issue exposes expressive/associational material, and possibly communications about the health and immigration status of family members, to unlimited government examination—and is therefore fatal to the constitutionality of the warrants both under the particularity inquiry and Fourth Amendment reasonableness generally.

II. The First Amendment Bars Enforcement of the Search Warrant to Obtain Facebook Messages from Members of the Public, Lists of Facebook Users Who Administer or Edit the FreeThemAllVa Page, and Lists of People Who Have Either "Liked" or "Followed" That Page.

The First Amendment provides an additional reason why the Government should not be given access to the identities of the individuals who administer or edit the FreeThemAllVA page, who have sent messages to the page, or posted comments on the page, or "liked" or "followed" the page. Merely providing the Facebook account names of members of the public who posted comments, who administer or edit or have"liked" or "followed : the FreeThemAll VA page, would likely identify the holders of those accounts because Facebook follows a "real name" policy, forbidding users from employing pseudonyms in creating their accounts.

A. First Amendment scrutiny limits court orders and government investigations that trench on First Amendment interests.

Court orders directed at private parties are governmental actions that are subject to scrutiny under the First Amendment. *NAACP v. Alabama*, 357 U.S. 449, 462 (1958). Such scrutiny applies even when the orders are issued at the behest of private parties, whether the orders are awards of

damages, *New York Times Co. v. Sullivan*, 376 U.S. 254, 265 (1964), or injunctive orders that compel private parties to take specific actions on pain of contempt. *Organization for a Better Austin v. Keefe*, 402 U.S. 415, 418 (1971). First Amendment scrutiny is all the more important where the order is sought from a court at the behest of government officials whose actions are themselves subject to the First Amendment's strictures. *NAACP*, 357 U.S. at 460-463; *New York Times Co. v. United States*, 403 U.S. 713, 714 (1971).

Government investigations that impinge on First Amendment interests, either directly or through their chilling effect, are subject to scrutiny under the First Amendment. *Gibson v. Florida Legis. Investigation Comm.*, 372 U.S. 539, 544 (1963); *NAACP*, 357 U.S. at 460-462. For example, in *Clark v. Library of Congress,* 750 F.2d 89 (D.C. Cir. 1984), the D.C. Circuit reversed the dismissal of a claim by an employee of the Library of Congress objecting to the fact that the Library had instigated an FBI full field investigation after it learned that he had attended meetings of the Young Socialists Alliance. Similarly, in *White v. Lee*, 227 F.3d 1214, 1238 (9th Cir. 2000), the Ninth Circuit allowed local critics of a proposed housing project to pursue First Amendment claims against federal housing officials for violating the critics' free speech rights by conducting a lengthy and intrusive investigation into their opposition. *See also ILA Local 1814 v. Waterfront Comm'n of New York Harbor*, 667 F.2d 267, 272 (2d Cir. 1981) (limiting state commission's demand for list of contributors to a political committee); *Donahoe v. Arpaio*, 986 F. Supp. 2d 1091, 1135 (D. Ariz. 2013) (denying summary judgment against civil rights claim alleging a retaliatory law enforcement investigation directed at dissenters); *Alliance to End Repression v. City of Chicago*, 627 F. Supp. 1044, 1050-52 (N.D. Ill. 1985) (allowing First Amendment claims to proceed where local law enforcement infiltrated certain groups and accumulated "an extensive dossier" about an individual);

Paton v. La Prade, 469 F. Supp. 773 (D.N.J. 1978) (allowing First Amendment claim brought by student over a "mail cover" that led to government recordation of his name and address as someone who had sent a letter to a socialist group so that he could write a school paper). Once the investigation was found to implicate First Amendment interests, these courts required the government to show that their investigations were justified under a standard of "exacting scrutiny."

Cases from both state and federal courts apply First Amendment limits to discovery orders in civil proceedings that seek information privileged against production by the First Amendment. In *Wyoming v Department of Agriculture*, 208 F.R.D. 449, 454-455 (D.D.C. 2002), for example, the court invoked First Amendment principles to limit discovery into materials protected by the First Amendment, requiring the parties seeking that discovery to show that the discovery they sought was central to their litigation contentions and that they had exhausted alternate means of obtaining the information they needed to advance their cases. *See also Zerilli v, Smith*, 656 F.2d 705, 714 (D.C. Cir. 1981), *United States v. Garde*, 673 F. Supp. 604, 607 (D.D.C. 1987); *Solers v. Doe*, 977 A.2d 941, 956 (D.C. 2009); *Independent Newspapers v. Brodie*, 407 Md. 415, 966 A.2d 432 (2009); *Mobilisa, Inc. v. Doe*, 217 Ariz. 103, 170 P.3d 712, 717 (Ariz. App. 2007); *Doe v. Cahill*, 884 A.2d 451, 456 (Del. 2005).

Although civil discovery orders trenching on the exercise of First Amendment rights have received the greatest judicial attention, discovery orders in criminal investigations have similarly been subjected to First Amendment scrutiny requiring the government to show "a compelling state interest in the subject matter of the investigation and a sufficient nexus between the information sought and the subject matter of the investigation." *In re Faltico*, 561 F.2d 109, 111 (8th Cir. 1977). *See In re Grand Jury Subp. No. 11116275*, 846 F. Supp. 2d 1, 4 (D.D.C. 2012). A leading case in

that line of authority is *Bursey v. United States*, 466 F.2d 1059, 1082 (9th Cir. 1972), where the Ninth Circuit limited a grand jury subpoena issued in the course of an investigation of the Black Panther Party, a political group whose policies included advocacy of violent self-defense of black communities against police intervention. Although the Court of Appeals found that the overall investigation was legitimate, it protected subpoenaed witnesses from having to answer certain questions that trenched too far on protected First Amendment interests and were insufficiently justified by the government's proffered explanation for its investigation. Similarly, in *Ealy v. Littlejohn*, 569 F.2d 219, 229 (5th Cir. 1978), when a grand jury investigating the murder of a local youth was used as an excuse to demand information about a local political group, the Fifth Circuit blocked the inquiry: "It 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." *See also Rich v. City of Jacksonville*, 2010 WL 4403095, at *11 (M.D. Fla. Mar. 31, 2010) (local law enforcement official who used subpoena power to identify anonymous blogger without having evidence of a crime denied qualified immunity in action for violation of blogger's First Amendment rights).

B. The First Amendment Limits Court Orders That Trench on the Right to Speak and Read Anonymously.

The search warrant in this case unduly intrudes into both the right to speak anonymously and the right to read anonymously. Both the United States Supreme Court and the Virginia Supreme Court have held that the First Amendment protects the right of authors to publish anonymously about political issue. *E.g.*, *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341-42 (1995); *Jaynes v.*

Commonwealth, 666 S.E.2d 303, 313 (Va. 2008). In *Jaynes*, the Virginia Supreme Court held that a Virginia statute compelling members of the public engaged in political speech to expose their identities to possible public disclosure by using accurate Internet Protocol addresses ("IP addresses") that could lead to disclosure of their actual names, by criminalizing the use of spoofed IP addresses for political communications, infringed the First Amendment right to speak anonymously and thus could be upheld only if it was "is narrowly drawn to further a compelling state interest." 666 S.E.2d at 312. The search warrant affidavit in this case establishes a compelling state interest in obtaining access to the live-streamed video and photographs of the demonstration in Leesburg during which a slogan was painted on a public sidewalk. However, the affidavit does not establish any compelling state interest in compelling disclosure of the other electronic records demanded by the search warrant, such as the messages sent by members of the public to the owners of the Facebook page, or the names, IP addresses and other information about Facebook subscribers who administer or edit the page, or who have commented on the page, or have liked or followed the page..

Moreover, it is "well established that the Constitution protects the right to receive information and ideas." *Stanley v. Georgia*, 394 U.S. 557, 564 (1969). This right "follows ineluctably from the **sender's** First Amendment right," and "[m]ore importantly, . . . is a necessary predicate to the **recipient's** meaningful exercise of his own rights of speech, press, and political freedom." *Bd. of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico*, 457 U.S. 853, 867 (1982) (plurality opinion) (emphases in original). "The dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers." 381 U.S. 301, 308 (1965) (Brennan, J., concurring); *see also Reno v. ACLU*, 521 U.S. 844, 874 (1997) (invalidating provisions of law that

"effectively suppresse[d] a large amount of speech that adults have a constitutional right to receive and to address to one another").

Just as the First Amendment right to speak includes the right to speak anonymously and provides protection against discovery, as discussed above, state and federal courts have recognized the right to read anonymously and have, accordingly, refused to enforce discovery demands for the identification of readers when not supported by a compelling government interest that was linked with sufficient precision to the demanded identification. Thus, *Lubin v. Agora*, 389 Md. 1, 882 A.2d 833 (2005), rejected a demand by the Maryland Securities Commissioner for the production of the list of subscribers to a financial newsletter; and *Tattered Cover v. City of Thornton*, 44 P.3d 1044 (Colo. 2002), restrained execution of a search warrant demanding that a bookstore produce customer records showing purchase of a "how to" book about producing drugs.

Two federal court decisions in the District of Columbia have applied the same principle. When Special Prosecutor Kenneth Starr served a grand jury subpoena on Kramerbooks demanding a list of Monica Lewinsky's purchases, the United States District Court for the District of Columbia recognized the First Amendment implications and demanded an in camera showing of the government's claim of a compelling justification. *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). In another case, that court limited grand jury subpoenas served in support of an investigation that was purportedly directed at obscene materials to seeking the identities of buyers of materials shown to be unprotected by the First Amendment. *In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq.*, 706 F. Supp. 2d 11, 18 (D.D.C. 2009). The lists of purchasers of expressive works of a sexual nature that were not shown to be outside First Amendment protection were

protected against compelled disclosure. *Id.* at 20-21.

And a different federal court, *In re Grand Jury Subpoena to Amazon.com Dated Aug. 7, 2006*, 246 F.R.D. 570, 572 (W.D. Wis. 2007), addressed a grand jury subpoena for a list of book buyers, issued in support of an otherwise legitimate investigation into whether a particular seller was engaged in mail or wire fraud. The court quashed the subpoena because of the chilling effect of identifying book buyers who were themselves accused of no wrongdoing to the government without their consent. Instead of ordering production of the list of buyers, Amazon, which had received the subpoena, was allowed to inform a subset of the customers in question of the investigation and ask them whether they would be willing to communicate with the prosecutors. The court ordered that Amazon provide the names only of those users who were willing to speak to the government, explaining:

> The subpoena is troubling because it permits the government to peek into the reading habits of specific individuals without their prior knowledge or permission. . . . [I]t is an unsettling and un-American scenario to envision federal agents nosing through the reading lists of law-abiding citizens while hunting for evidence against somebody else. [In an era of pervasive surveillance and politicized Justice Department applying litmus tests,] rational book buyers would have a non-speculative basis to fear that federal prosecutors and law enforcement agents have a secondary political agenda that could come into play when an opportunity presented itself. Undoubtedly a measurable percentage of people who draw such conclusions would abandon online book purchases in order to avoid the possibility of ending up on some sort of perceived "enemies list."
>
> *Id.* at 572-573.

The right to speak anonymously, the right to read anonymously, and the right to engage in anonymous political association are each implicated here. To the extent that third-party Facebook holders have either placed comments on the FreeThemAllVa page, or sent private messages to the page, their communications are speech subject to First Amendment protection. The act of "liking"

a Facebook page or a Facebook posting is a form of speech subject to First Amendment protection. *Bland v. Roberts*, 730 F3d 368, 385-386 (4th Cir. 2013). Moreover, "liking" and "following" are not just means of expressing approval—they can also serve as a means of subscribing to notifications of additional posting to the "liked" or "followed" page. Thus, the list of likers and followers is comparable to the lists of buyers or subscribers that were protected against criminal discovery in such cases as *Lubin*, *Tattered Cover*, and *Amazon*. Finally, the lists of followers and likers are also lists of association members comparable to the lists that were subject to protection against compelled disclosure in *NAACP v. Alabama*, 357 U.S. at 462, and *Bates v. Little Rock*, 361 U.S. 516 (1960). For all these reasons, the likers, followers and authors of comments and Facebook messages are all protected against identification by court order absent compelling justification.

C. The Commonwealth has not made a showing of compelling need to identify the hundreds of Facebook account holders who have "liked" or "followed" the Free Them All VA Facebook or acted as administrators or editors of the page, or posted comments on or sent messages to that page.

The implications of the Court allowing a police department to compel the identification of more than a hundred Facebook account holders who liked or followed the FreeThemAllVa page, or who sent written communications either through Facebook's messaging procedures or by posting on the page, are chilling indeed. Intrusion into the privacy of so many individuals who associated anonymously with a page advocating for those incarcerated in Virginia should not be enforced without a highly exacting showing of the government's need for that information.

The affidavits of the Doe intervenors explain the innocent, constitutionally protected reasons for associating with this Facebook page. One hundred fifty members of the public have "liked" or "followed" the FreeThemAllVA page, whether to express support for the organization, or to have

a convenient way to receive notification when new events or changes in existing events were posted, or for both reasons. Members of the public who were connected to the pages in question posted comments to initiate discussions about a variety of political issues, and to participate in such discussions. The government has no legitimate basis for gaining access to any of these communications, and no compelling interest in identifying the individuals who engaged in this protected First Amendment activity.

Indeed, a Virginia statute has imposed procedural requirements before discovery is allowed to identify anonymous Internet speakers in civil proceedings: the party seeking discovery must supply the court with the evidence and argument on which it relies as a basis for divesting an Internet user of anonymity, and serve that filing on the Internet Service Provider ("ISP") from whom identifying information will be sought; the ISP must provide that information to all users whose anonymity is at stake; the anonymous user may appear as a Doe to argue for the protection of her anonymity; and the court must decide whether the party seeking discovery has made a sufficient showing to overcome the First Amendment right to speak anonymously. Virginia Code § 8.01–407.1. *See Yelp, Inc., v. Hadeed Carpet Cleaning,*, 770 S.E.2d 440 (Va. 2015).

The Court should be very cautious about allowing a police department to search the electronic files of an opposition group on a minimal showing of probable cause. Particularly in this context, the very fact of searching the entire set of messages sent to Facebook page putatively promoting nonviolent protest, sweeping into the government's net the identities of people not connected to the page who did no more than communicate to try to obtain more information or to offer support, will inevitably have a serious chilling effect that offends the First Amendment. *See NAACP v. Alabama*, 357 U.S. at 462; *In re Grand Jury Subpoena to Amazon.com Dated Aug. 7,*

2006, 246 F.R.D. 570, 572 (W.D. Wis. 2007).

If the subpoena is not quashed entirely, Movants urge the Court to impose procedural limitations on the Leesburg Police Department's access to identifying information connected with specific communications found to be truly needed for the investigation of the alleged crime that is being investigated in this case, similar to those imposed by the "three-step process" adopted by the court in *DisruptJ20*, discussed above.[1] That is, Facebook should be directed to provide access to the records of the FreeThemAllVA account with identifying information about other Facebook account holders redacted. The Commonwealth should be required to provide the Court with a search protocol for reviewing communications between the FreeThemAllVA page and members of the public, and to refrain from searching those communications until the Court has approved the search protocol. Then, after conducting the search, the Commonwealth should be required to present a statement of reasons why each communication is within the scope of the probable cause supporting the warrant. And only at that stage should the Commonwealth be given an opportunity to make a showing of its need for identifying information with respect to the sender or recipient of a given communication.

CONCLUSION

The motion to quash should be granted.

Respectfully submitted,

/s/ Nina J. Ginsberg

[1] Identification of Facebook users who had "liked" the DisruptJ20 page, or who had "friended" individual Facebook users whose accounts were also subject to warrants, was no longer at issue because, in response to a motion to quash filed by Facebook users who had "liked" or "friended" the accounts at issue, the government agreed to narrow its search warrant by excluding a demand for identifying information about "likers" or "frienders."

Nina J. Ginsberg (Va. Bar 19472)

DiMuro Ginsberg, PC
Suite 610
1101 King Street
Alexandria, Virginia 22314-2956
(703) 684-4333 (telephone)
(703) 548-3181 (facsimile)
(703) 623-6975 (cellular)
nginsberg@dimuro.com

/s/ Paul Alan Levy
Paul Alan Levy (D.C. Bar 946400)
(pro hac vice to be sought)

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

Attorneys for Doe Movants

October 13, 2020