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 Robert E. Morin

ORDER

This matter comes before the court pursuant to the government's motion to show cause seeking to compel Facebook, Inc. ("Facebook") to comply with three search warrants issued by the court on February 9, 2017, Nos. 17 CSW 658, 17 CSW 659, 17 CSW 660 (hereinafter, the "Warrants" or "February 2017 Warrants"), and Facebook's opposition thereto, along with the motions to intervene filed by Lacy Macauley, Legba Carrefour, and Emmelia Talarico (collectively, "the account holders") and the government's opposition thereto.

I. BACKGROUND

On February 9, 2017, the court (Wertheim, J.) authorized three separate search warrants[1] for the Facebook accounts DisruptJ20, lacymacauley, and legba.carrefour, having found probable cause that each account contained evidence of violations of D.C. Code § 22-1322 (rioting or inciting to riot) that occurred on January 20, 2017, in connection with the presidential

[1] The Warrants were issued pursuant to 18 U.S.C. §§ 2703 (a), 2703 (b)(1)(A) and 2703 (c)(1)(A) of the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701, *et seq.*, which authorizes the government to compel disclosure by a service provider, here Facebook, for all records and all email communications in a particular account. An SCA warrant is issued using the applicable state warrant procedures (*id.* § 2703 (a); *see* D.C. Super. Ct. Crim. R. 41), and can generally be executed without notice to the subscriber. *Id.* § 2703 (b)(1)(A).

inauguration ("January 20 riots"). At the same time, the court issued three non-disclosure orders directing Facebook to temporarily delay notice of the Warrants to the account holders.

In response, Facebook withheld production and challenged the appropriateness of the non-disclosure orders. After hearing argument by both parties, the court declined to lift the non-disclosure orders. Facebook appealed the decision to the Court of Appeals, and oral argument was scheduled for September 14, 2017. On September 13, 2017, at the government's unopposed request, this court issued an order vacating the non-disclosure orders associated with each of the subject Warrants. Facebook then dismissed its appeal as moot.

Shortly thereafter, Facebook notified the account holders of the existence of the Warrants and provided them with an opportunity to bring their own challenge. The account holders moved to intervene and quash or narrow the Warrants on September 28, 2017. The government filed its opposition on October 4, 2017, arguing that the account holders' motion is premature because the Warrants have not yet been executed, and therefore, the account holders have no right to bring a challenge. The account holders filed their declarations and reply on October 10, 2017, and the court heard argument by all parties on October 13, 2017. To date, Facebook has not produced any data to the government, contending that it should not be required to comply until the account holders' motions are fully adjudicated.

Facebook Search Warrants

It is undisputed that the Warrants are directed to two individual Facebook accounts ("the individual accounts") and one Facebook Page ("the Page"), for which the court found probable cause contained evidence of alleged crimes committed in the District of Columbia in violation of D.C. Code § 22-1322 by individuals for which the Grand Jury has already indicted over 200 people.

Execution of the Warrants will require Facebook to provide the government with extensive information for each targeted account, including the contact and personal identifying information for each account holder, and all profile information, activity logs, wall posts, notes, comments, photos, videos, friend lists, organizers and attendees for sponsored events, groups and networks joined, Facebook searches, deleted data, rejected friend requests, blocked friends, chats, live streams, and direct and group Facebook Messenger communications between the account holders and those with whom they communicated. Data to be produced under the Warrants is limited to approximately three months (between November 1, 2016 and February 9, 2017).

Some of the information sought is not publicly available and access to communications on the individual accounts and the Page is limited to particular individuals. In addition, based on proffers by the account holders and other third parties, the data may include deeply personal information (e.g., family pictures, details of romantic relationships, domestic violence encounters, and communications regarding medical and psychiatric history) and contain protectable political speech and association (e.g., political commentary, affiliations, names and pictures of event organizers and attendees) unrelated to the January 20 riot.

The Warrants, as issued, did not include any limiting safeguards to explain how the government would compel the production of data containing criminal evidence, or how the government intended to search the data received. Rather, the Warrants indicated that, after the government receives all data for the targeted accounts, it would only "seize" data relevant to information that it believes evidences the alleged crimes, as set forth in the supporting

Affidavits.[2] Subsequently, the government modified its request and indicated that it will remove any non-pertinent information from its possession.

Accordingly, in line with the traditional two-step process, the government requests that all information responsive to the Warrants be disclosed, but commits that it will ultimately not retain material non-pertinent to its investigation.

II. ANALYSIS

A. The February 2017 Warrants

The First Amendment broadly protects the right to engage in anonymous political speech and associational activity. *See McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341 (1995) ("[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."); *NAACP v. Alabama*, 357 U.S. 449, 462 (1958) ("compelled disclosure of affiliation with groups engaged in advocacy may constitute [an] effective [] restraint on freedom of association"). First Amendment freedoms are no less robust on the internet. *See Reno v. ACLU*, 521 U.S. 844, 870 (applying the First Amendment to the internet); *Solers, Inc. v. Doe*, 977 A.2d 941, 950-51 (D.C. 2009) ("[a]nonymous internet speech in blogs or chat rooms in some instances can become the modern equivalent of political pamphleteering") (citation omitted); *see also Bland v. Roberts*, 730 F.3d 368, 385-86 (4th Cir. 2013) (holding that "liking" a Facebook page or wall post is a form of protected speech). Protecting a speaker's right to conceal their identity is grounded in an "honorable tradition of advocacy and dissent," *McIntyre*,

[2] Because the February 2017 Warrants were issued as part of a Grand Jury investigation, the Affidavits are sealed under D.C. Super. Ct. Crim. R. 6 (e) and have not been disclosed (full or redacted) to Facebook or the account holders.

514 U.S. at 357, and necessary to ensure that public debate is "uninhibited, robust, and wide-open." *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964).

The Supreme Court has determined that, when the government's investigation intrudes on First Amendment activity, the requirements of the Fourth Amendment must be applied with "scrupulous exactitude." *Stanford v. Texas*, 379 U.S. 476, 485 (1965); *accord, Maryland v. Macon*, 472 U.S. 463, 468 (1985). The right to be free from government intrusion is preserved even where the government does not intend to cause specific harm. *See Lyng v. Int'l Union*, 485 U.S. 360, 367 n.5 (1988). Hence, the government must show that it has a compelling interest to justify even a subtle interference with an individual's ability to freely associate. *See NAACP*, 357 U.S. at 463.

Electronic searches can be time-consuming and raise logistical difficulties for law enforcement tasked with locating specific criminal evidence amidst all information in a given storage medium. In recognition of these difficulties, Superior Court Criminal Rule 41 (e)(2)[3] presumptively authorizes a two-step process by which law enforcement may conduct "a later review of the media or information consistent with the warrant."[4] This rule is substantially identical to its federal counterpart, Fed. R. Crim. P. 41 (e)(2)(B), as amended in 2009.[5]

---

[3] Super. Ct. Crim. R. 41 (e)(2) sets forth the procedural requirements for obtaining a warrant seeking electronically stored information.

[4] "A warrant under this rule may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in this rule refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." Super. Ct. Crim. R. 41 (e)(2).

[5] Rule 41 (e)(2)(B) approves a two-step process for the search and seizure of electronically stored information. The Advisory Committee Notes further discuss the need for such a process:

Courts have generally agreed that a two-step process is appropriate for searches of computers or hard drives, often containing substantial information, to ensure that evidence is properly preserved.[6] *See, e.g., In the Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.,* 13 F. Supp. 3d 157, 166 (D.D.C. 2014) ("*In re Apple Account*") (authorizing government's seizure of defendant's home computer and digital media for a subsequent off-site electronic search where there was a "fair probability" of finding evidence on those devices) (following *United States v. Schesso*, 730 F.3d 1040, 1046 (9th Cir. 2013); *United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012) ("The federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a 'sufficient chance of finding some needles in the computer haystack.'") (quoting *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999)).

> Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant . . . [E]lectronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location.

Fed. R. Crim. P. 41 (e) Advisory Committee's Note (2009).

[6] Searches of electronic storage media commonly require "time-consuming electronic forensic investigation with special equipment" to account for the countless ways of hiding evidence on the device. *United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017). Because the amount of information make it impractical for law enforcement to search the device at the location where it was seized, Rule 41 (e)(2) allows officers to copy the entire medium and review it later off-site to both enable execution of the search and prevent the destruction of information on the computer. *See United States v. Stabile*, 633 F.3d 219, 234 (3d Cir. 2011) (stating that the "practical realities of computer investigations preclude on-site searches").

The court acknowledges the usefulness of a two-step process. At the same time, it is certainly true that electronic searches may present increased risks to the individual's right to privacy and other constitutional interests "as technological advances enable law enforcement to monitor and collect large volumes of electronic communications and other data." *In re Apple Account*, 13 F. Supp. 3d at 166; *see United States v. Blake*, 868 F.3d 960, 973-74 (11th Cir. 2017) (noting that application for an individual's entire Facebook account would unnecessarily disclose to the government "virtually every kind of data"). Courts have acknowledged that, with such large disclosures of data, the government will inevitably come across unrelated material that exceeds the scope of the warrant. *See Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."); *United States v. Sealed Search Warrant*, 2017 U.S. Dist. LEXIS 125792, at *13 (N.D. Ala. Aug. 8, 2017) (acknowledging that "some perusal" is generally necessary to determine the "relevance of documents to the crime") (quoting *United States v. Slocum*, 708 F.2d 587, 604 (11th Cir. 1983)). As "over-seizing" is considered to be an "inherent part of the electronic search process," it often provides the government with "access to a larger pool of data that it has no probable cause to collect." *In re Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis*, 21 F. Supp. 3d 1, 8 (D.D.C. 2013) ("*Aaron.Alexis*").

Today's ever-accelerating technological advances are transforming the way people interact with the world around them, often leaving the user's privacy expectations trailing slowly behind. The interactive nature between digital devices and use of social media means more personal details that were once kept in private diaries, or computers, are now being stored with third party data storage companies. The natural consequence of living in a highly connected age,

however, is the substantial likelihood that a subscriber's intimate personal information can be discovered by an unintended recipient. Privacy is an evolving concept in the online context, where subscribers are often free to choose their own privacy settings for their online accounts, ranging from completely private (accessible only to user) to limited (between user and specific individuals) to public. This analysis gets even more complicated when determining how much government access should be afforded.[7] Pervasive use of "cloud " technology and social media, combined with growing online storage capacities,[8] creates "a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *In re Cunnius*, 770 F. Supp. 2d 1138, 1151 (W.D. Wash. 2011); *accord, United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc).

Due to the individual interests implicated in electronic searches— particularly those searches involving lawful political activity and expression—the Supreme Court has tasked judicial officers with the responsibility of ensuring that electronic searches "are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Andersen*, 427 U.S. at 482 n.11. As a result, courts have wrestled with how to balance an individual's right to engage in private online expression with the government's ability to prosecute criminals, especially where probable cause has been established that a particular electronic device or online account may contain evidence of a criminal offense. *See, e.g., In re Info. Associated with @gmail.com*, 2017

---

[7] Although unresolved in the District of Columbia, the Sixth and Ninth Circuits have afforded electronic communications the same Fourth Amendment privacy protections as their offline counterparts. *See In re Google Account*, 2017 U.S. Dist. LEXIS 130153, at *17 n.13 (citing *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010)); *In re Grand Jury Subpoena*, 828 F.3d 1083, 1090 (9th Cir. 2016).

[8] For example, "a single gigabyte of storage space is the equivalent of 500,000 double-spaced pages of text." *In re Cunnius*, 770 F. Supp. 2d at 1144.

U.S. Dist. LEXIS 130153, at *77 (D.D.C. July 31, 2017); *United States v. Search of Info. Associated with Fifteen Email Addresses*, 2017 U.S. Dist. LEXIS 159535, at *19-23 (M.D. Ala. Sept. 28, 2017) ("*Fifteen Email Addresses*"); *In re Search of Info.*, 212 F. Supp. 3d 1023, 1038 (D. Kan. 2016). This means that determinations must be made on a case-by-case basis. *Schesso*, 730 F.3d at 1046.

The risk for disclosure of private political speech and association of innocent persons to the government cannot be ignored and therefore additional protections are necessary. Various courts have agreed that, although not required by the Fourth Amendment, incorporating additional protections into electronic search warrants are appropriate to minimize the possibility of abuse by the government. *See In re Search of Info.*, 212 F. Supp. 3d at 1038 (acknowledging "that a judge may have the authority to impose reasonable *ex ante* instructions"); *United States v. Christie*, 717 F.3d 1156, 1166-67 (10th Cir. 2013) (discussing that the particularity requirement may or may not require limitations *ex ante*); *In re Search Warrant*, 71 A.3d 1158, 1186 (Vt. 2012) (rejecting "any blanket prohibition on *ex ante* search warrant instructions") ("*Vt. Search Warrant*"); *United States v. Hill*, 459 F.3d 966, 976-77 (9th Cir. 2006) ("[W]e look favorably upon the inclusion of a search protocol; but its absence is not fatal."). In some circumstances, restrictions have been viewed as "essential to meet the particularity requirement of the Fourth Amendment," especially where, as here, the search involves nonresponsive information intermingled with relevant evidence. *Vt. Search Warrant*, 71 A.3d at 1184. In fact, the federal courts in the District of Columbia have often required the government to implement search protocols into its warrant applications to minimize the risk that non-pertinent data is discovered. *See, e.g., In re Search of Apple iPhone*, 31 F. Supp. 3d 159, 164 (D.D.C. 2014) ("*Apple iPhone*") (requiring the government to explain how it intends to conduct its search and deal with issue of intermingled documents); *In re Search of ODYS LOOX Plus Tablet*, 28 F. Supp. 3d 40, 46 (D.D.C. 2014) ("No sophisticated search should occur without a detailed explanation of the methods that will be used, even if the explanation is a technical one,

and no search protocol will be deemed adequate without such an explanation."); *Aaron.Alexis*, 21 F. Supp. 3d at 11-12 (outlining non-exhaustive minimization plan for electronic searches).[9]

Although the online presence of individuals is more prevalent, current technological capabilities allow law enforcement in some circumstances to execute electronic searches of online email and social media accounts in a more targeted manner than is possible on a hard drive or computer. *See Fifteen Email Addresses*, 2017 U.S. Dist. LEXIS 159535, at *16-18 ("[S]orting the main content—emails—by date or sender or recipient or even by keyword would be much easier than sorting data stored on a hard drive."); *Apple iPhone*, 31 F. Supp. 3d at 161 ("By using search tools, there is also the potential for narrowing searches so that they are more likely to find only the material within the scope of the warrant."); *In re A Warrant for All Content & Other Info. Associated with the Email Account xxxxxx@Gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014) ("Indeed, in many cases, the data in an email account will be less expansive than the information that is typically contained on a hard drive."); *see also 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."). Unlike searches of computers or hard drives, "the means of hiding evidence . . . [through] obscure folders, misnamed files, [or] encrypted data[, is] not currently possible in the context of a Facebook account." *Blake*, 868 F.3d at 974.[10] In fact, for Facebook

[9] The search protocols included: (1) limiting searches to specific keywords or between particular recipients; (2) appointing a special master to screen the responsive information for relevance and privilege; (3) setting up a filter group or taint team to review the information for relevance and privilege; (4) waive reliance on the plain-view doctrine; and (5) the incorporation of search protocols designed to reveal only the information for which the government has probable cause to seize. *Aaron.Alexis*, 21 F. Supp. 3d at 11-12.

[10] The variety of services linked to an e-mail account (email storage, calendar, pictures, files, videos, cloud capabilities) can provide "more ways to hide things . . . than on Facebook," but still less than a hard drive. *Fifteen Email Addresses*, 2017 U.S. Dist. LEXIS 159535, at *17.

account searches, "the government need only send a request with the specific data sought and Facebook will respond with precisely that data." *Id.* Such requests can feasibly be narrowed to particular individuals suspected of taking part in the alleged crime, or where unknown, limiting data production by types of files or communication topics. *Fifteen Email Addresses*, 2017 U.S. Dist. LEXIS 159535, at *22; *United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006).

There are circumstances in this case which allow the court to consider limitations on the government's search while also protecting its legitimate need to prosecute criminal activity. Here, the information sought by the February 2017 Warrants has been preserved by Facebook so that there is no risk of its destruction. In addition, by agreement of the government, the account holders and other third parties have been provided notice and an opportunity to present argument on the issue. And, finally, Facebook currently has the technological capabilities to enable execution of the Warrants in a manner that also protects innocent users' privacy and First Amendment interests.

Based on the current proffers, execution of the Warrants will produce to the government a variety of data and communications associated with the two individual accounts and the Page. Any evidence in the production of data will likely be co-mingled with personal information and otherwise protected political and associational material, implicating the privacy and First Amendment rights of the account holders and other third parties who interacted or communicated with the targeted accounts. Given the potential breadth, the Warrants in their execution may intrude upon the lawful and otherwise innocuous online expression of innocent users. Therefore, the court deems it appropriate in this case to implement procedural safeguards to preserve the First Amendment and Fourth Amendment freedoms at stake and ensure that only data containing potential incriminating evidence is disclosed to the government.

B. Procedural Safeguards

As this court has previously stated in a similar context, while the government has the right to execute its warrants, it does not have the right to rummage through the information contained on the Facebook accounts and discover the identity of, or access communications by, individuals not participating in alleged criminal activity, particularly those persons who were engaging in protected First Amendment activities. *In the Matter of the Search of www.disruptj20.org That Is Stored at Premises Owned, Maintained, Controlled, or Operated by DreamHost*, No. 17 CSW 3438, at *1 (D.C. Super. Ct. Oct. 10, 2017) ("*DreamHost*").

The Warrants that are directed to the two individual Facebook accounts are distinguishable from the Facebook Page. The Page is similar to the website this court addressed in *DreamHost*, with multiple persons having access to, and communicating through, a common forum. *See id.* In contrast, the individual accounts are more analogous to an email account which historically has been subject to authorized search warrants without limitations, together with other stored data, some of which is intended to be publicly available and some of which is intended to be private.

Because of the different nature of the Page and the individual accounts, the government's search of each must be tailored to the nature of the data being stored and account for what was intended to be private and that which was not. Accordingly, the court sets forth protections that must be adhered to in searching the Page, followed by the protocols for searching the individual accounts. Law enforcement will be able to feasibly execute these safeguards based on Facebook's technological capabilities.

Facebook Page (DisruptJ20)

In line with the government's representations at the October 13 hearing, the government's request for information relating to the Page has been narrowed to (1) exclude from production the identities of any individuals who liked or followed the Page, and (2) limit the production of any photographs uploaded (between January 20, 2017 and February 9, 2017).

The government also agreed to narrow its warrant for the Page by implementing the search protocol ordered by this court in *DreamHost*, No. 17 CSW 3438. In accordance with the *Dreamhost* order, the government must adhere to the following safeguards:

1. File a report with the court, *ex parte* and under seal,[11] explaining the government's intended search protocols designed to uncover only that data and information that evidences the alleged crimes that serve as the basis for the Warrant at issue;
2. If the court approves the protocols, the government may only conduct its search on a redacted data set that omits non-account holder identifying information;[12]

---

[11] The court determines that it is appropriate for the government to submit its report *ex parte* and under seal because the government's criminal investigation is ongoing and may be hindered by public disclosure at this time.

[12] In a subsequent filing, dated October 20, 2017, Facebook informed the parties and the court that it currently lacks the technology to automatically redact user identification information, or separate communications, postings, etc. for which the privacy setting was accessible to the general public when made. *See* Facebook Tech. Capabilities 1-2. It is beyond dispute that persons who post information or communicate publicly would not have a reasonable expectation of privacy protectable by the Fourth Amendment. Thus, if it were technologically possible, the court would order that Facebook provide the "public" data to the government without limitation. Yet, this is not an option given the technological limitations proffered by Facebook.

Nevertheless, Facebook has indicated its willingness to manually redact the user identification information set for private, but that effort would likely take three weeks. *Id.* Upon completion of any redactions, as discussed at the October 13 hearing, Facebook shall produce to the government a redacted data set—i.e., all information for each account that is responsive to the Warrants, having manually redacted any identifying information of all persons—other than Facebook account holders—who communicated with an individual account or the Page at issue.

3. Upon completion of review, the government must file with the court, *ex parte* and under seal, an itemized list of the materials it believes evidences a violation of D.C. Code § 22-1322, explaining how such materials are relevant to its investigation, its basis for removing any redactions, and how it will permanently remove from its possession any non-pertinent data; and
4. Only upon a finding by the court that the requested information is evidence of criminal activity, as described in the Warrant for which this court has found probable cause, may the government obtain any un-redacted information, such as the identity of a third party user.

DreamHost, No. 17 CSW 3438, at *2, *5-10. The government shall not begin its review of the redacted materials provided by Facebook until the court has approved the government's proposal and authorized the government to begin its detailed review of the redacted materials.

Individual Accounts (Lacymacauley and Legba.Carrefour)

At the October 13 hearing, the government indicated that it seeks to conduct a "front-to-back" (rather than "key word") search with respect to the individual accounts. The government also narrowed the information sought by (1) excluding from production the list of friends of an individual account, (2) excluding from production the identities of any individuals who liked or communicated with an individual account, and (3) limiting the production of all photographs uploaded to a particular individual account (between January 20, 2017 and February 9, 2017).

Because the communications and records sought relate to specific individuals, and the government has established probable cause as to those individuals, the government is authorized to review the communications and postings in the individual accounts. Having already

---

Such redactions shall remain in place until such time as the court in the exercise of its discretion directs Facebook to remove any of those redactions.

established probable cause to believe that criminal activity is likely to be found in the individual accounts, the government is entitled to review the material and determine for itself whether, and to what extent, there is evidence of criminal activity.

Assuming that any alleged evidence is intermingled with unrelated information, that intermingling exists because the account holders chose to store their data with a third party, Facebook, in that manner. This is distinguishable from the information concerning persons whose information is sought due to their lawful interaction with the targeted accounts. Probable cause has not been established with respect to these individuals and thus they are entitled to remain anonymous.

To ensure that the identities of innocent persons are not revealed, the government must conduct its review in accordance with the following procedures:

1. Facebook shall redact any identifying information of persons to whom Facebook Messenger communications are sent, persons who liked or friended a particular account holder, and other information not directly related to an account holder.
2. Once the government has reviewed the redacted information, it shall file with the court, *ex parte* and under seal, any request(s) for non-redacted identifying information, including an explanation as to why a specific record should be revealed to the government.
3. The government must then permanently delete from its possession any data that does not fall within the authorized scope of the Warrants; and
4. The government shall not distribute, publicize, or otherwise make known to any other person or entity, to include any other law enforcement or government entity, the data and information not within the authorized scope of the Warrants.

The Court reiterates that the government can always seek additional warrants if it later determines that its search was too narrow.[13]

C. Motion For Account Holders To Intervene For A Limited Purpose

The account holders moved to intervene for the limited purpose of challenging the Warrants directed at their personal Facebook accounts and the Facebook Page,[14] arguing infringement of both their Fourth Amendment right to privacy in their personal information and First Amendment right to political speech and association. Movants claim that, because execution of the Warrants would disclose to the government their private and political information which cannot be later undone, they should be permitted to challenge the Warrants *ex ante* to preserve their interests and any appeal rights.[15]

The parties do not dispute that D.C. Rules of Criminal Procedure do not explicitly allow a non-party to challenge a search warrant prior to its execution. Movants point to Criminal Rule 57 (b), which provides that "when there is no controlling law[, t]he court may regulate practice in any manner consistent with applicable law and these rules." *See* Super. Ct. Crim. R. 57 (b). However, Criminal Rule 41 (g) directs that the appropriate remedy for an individual aggrieved

---

[13] *See Fifteen Email Addresses*, 2017 U.S. Dist. LEXIS 159535, at *10 ("The government is free to return and seek additional search warrants based on the new evidence it discovers.") (citation omitted).

[14] The court denies the request by the Jane and John Does to intervene since all identifying information, with the exception of the account holders, will not be disclosed to the government unless and until the court has determined that such information is evidence of criminal activity. Because it is not known whether the identity of the Does will ever be made known, intervention at this time is not appropriate.

[15] Disclosure could foreclose the opportunity for account holders to bring any motion for reconsideration or to appeal the decision. *See Bruce v. Potomac Electric Power Co.*, 162 A.3d 177, 183 (D.C. 2017) ("compliance with a subpoena will typically render an appeal from an enforcement order moot").

by a search he or she believes to be unlawful is to move to suppress evidence obtained as a result of that search. *See* Super. Ct. Crim. R. 41 (g).

In addition, although other courts have permitted non-party intervention *ex ante* for the limited purpose of addressing a specific issue, such interventions were under decidedly different circumstances. For example, the Court of Appeals has authorized the limited intervention of a non-party in a criminal proceeding to protect constitutional interests, *In re Jury Questionnaires*, 37 A.3d 879, 884 (D.C. 2012), or to secure access to court records. *Mokhiber v. Davis*, 537 A.2d 1100, 1144 (D.C. 1988). Courts have also allowed non-party intervention when the subject is seeking to prevent disclosure of his or her information on grounds of privilege. *See, e.g.*, *In re Search of Electronic Comm'n*, 802 F.3d 516, 529-30 (3d Cir. 2015) (granting pre-enforcement intervention of Google email account user challenging search warrant on non-constitutional grounds); *Doe No. 1 v. United States*, 749 F.3d 999, 1005 (11th Cir. 2014) (authorizing non-party intervention in criminal proceeding to challenge disclosure of privileged information); *In re Sealed Case*, 237 F.3d 657, 663-65 (D.C. Cir. 2001) (granting limited intervention under Civil Rule 24 (b) to subject of FEC investigation who had a legally cognizable interest in confidentiality of subpoenaed documents); *United States v. Hubbard*, 650 F.2d 293, 311 n.67 (D.C. Cir. 1980) (remanding denial of intervention by non-party seeking to prevent public access to documents on property and privacy interests).

Assuming intervention was authorized, however, the court nevertheless has discretion to determine whether movants should be entitled the opportunity to review the government's supporting Affidavits and to challenge disclosure of their information before the Warrants are executed. In exercising it discretion, the court considers a number of circumstances weighing in favor and against allowing intervention. For example, weighing in favor of intervention, there is

no risk of evidence destruction since Facebook has preserved all the relevant materials or risk of undue delay since the proceedings have already been delayed largely due to litigation surrounding the non-disclosure orders, which the government ultimately agreed to vacate. Weighing against intervention, there is a practical concern that granting a limited intervention would "open the floodgates to pre-execution warrant challenges" resulting in a strain on court resources. *In re [REDACTED]@gmail.com*, No. 14-M-1233, at *6 (E.D. Wisc. July 29, 2014). Likewise, allowing pre-execution intervention by movants would unduly compound litigation, making it protracted and frustrating the speedy resolution of investigations by the government.

As discussed, it is understood that the account holders and other Facebook users have a Fourth Amendment privacy right to their personal information. *United States v. Ali*, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012). They also have a First Amendment right to anonymously post on the internet, *In re Grand Jury Subpoena No. 11116275*, 846 F. Supp. 2d 1, 4 (D.D.C. 2011), and the right to be free from government interference. *See Lyng*, 485 U.S. at 367 n.5. Where First Amendment freedoms are directly at issue, the Supreme Court has held that intervention is appropriate to provide an opportunity for the affected individual to be heard. *Quantity of Books v. Kansas*, 378 U.S. 205, 210 (1964); *Marcus v. Search Warrant*, 367 U.S. 717, 734-38 (1961). Specific procedural protections, including pre-execution challenges, may also be appropriate where the government is seizing presumptively protected materials. *See Fort Wayne Books, Inc. v. Indiana*, 489 U.S. 46, 63-64 (1989) ("[t]he risk of prior restraint . . . is the underlying basis for the special Fourth Amendment protections accorded searches for and seizure of First Amendment materials") (citation omitted); *Connick v. Myers*, 461 U.S. 138, 145 (1983) ("speech on political issues occupies the highest rung of the hierarchy of First Amendment values, and is entitled to special protection"); *but see Heller v. New York*, 413 U.S. 483, 492-93

(1973) (denying pre-enforcement challenge where the targets of the search may destroy or move criminal evidence).

Although the search may implicate movants' privacy interests as to their personal information, in a legal sense such interests have already been taken into account by requiring the government to meet the higher burden, and correspondingly higher protections, involved in obtaining a search warrant. Subpoenas are generally subject to pre-enforcement challenges because they lack certain safeguards that are required in issuing a search warrant. Unlike subpoenas, search warrants generally are not subject to pre-enforcement challenge because the Constitution imposed specific procedural safeguards for issuing search warrants, such as issuance by a neutral, detached judicial officer and the establishment of probable cause, that are not required in issuing subpoenas. *In re Grand Jury Subpoena No. 11116275*, 846 F. Supp. 2d at 4 n.6. Here, the Warrants were issued after an impartial judicial officer found probable cause to believe that the individual accounts contained evidence of a criminal offense, as supported by a factual presentation by law enforcement which was sworn to oath or affirmation, and describing with particularity the scope of the search. Such a review process is not available when issuing a subpoena. Consequently, the court is hesitant to undermine the integrity of the impartial review that was already undertaken in this case by "wip[ing] the slate clean" through any substantive review of the account holders' requests challenging the Warrants *ex ante*. *In re [REDACTED]@gmail.com*, No. 14-M-1233, at *2, 6.

Moreover, the court has imposed additional safeguards to protect the privacy and legitimate expression by the account holders and other third parties interacting with the target accounts. Any identifying information about individuals who interacted with the target accounts (by being Facebook friends, liking or commenting on posts, following the Page, sending or

received Facebook Messenger communications to/from a target account) will be redacted and only revealed to the government upon express authorization by the court. Even if ultimately there is no evidence of criminal activity found in the individual accounts, the account holders' privacy interests will be preserved since the government is foreclosed from disclosing the contents of information that it has reviewed to any other person or entity.

In reality, given the unique posture of this case, the court has already received multiple pleadings and arguments from the account holders to which the government has had a full opportunity to respond. The court has conducted a full hearing, open to the public, to consider the account holders' issues and the government's opposition thereto. In that sense, the movants have been heard and their positions taken into account so that they have received the practical benefit that any formal intervention would provide. Indeed, their involvement in the proceedings, though unprecedented, has been informative in minimizing intrusion by the government into their own information while also ensuring that the identities of innocent users are protected.

Intervention is not favored where doing so would be futile. *Microsoft Corp. v. United States DOJ*, 233 F. Supp. 3d 887, 916 n.17 (W.D. Wash. 2017) ("[A] court need not grant leave to amend where amendment would be futile") (citation omitted). Since the account holders have had robust involvement before this court, the only conceivable benefit is a speculative opportunity to appeal this court's order, which the court does not determine to be a sufficient reason to circumvent the normal processes concerning the enforcement of search warrants.

In summary, the movants have been provided notice and an opportunity to protect their interests. In this case, because Facebook has not produced the information sought by the Warrants, the account holders have not yet been aggrieved by any unlawful search and thus have

no Rule 41 authority to challenge it. Perhaps more persuasive, however, is that the results of the government's search remain unknown at this time. In the event that the government seizes any data or information, there are specific remedies allowed for under Rule 41 (g) to which the movants may avail themselves, if and when that becomes appropriate. Pursuant to this court's order, any data not seized by the government will be destroyed and not disclosed to any other person or entity, including government entities. As a result, any private information will remain private. Thus, the traditional process of challenging the issuance or execution of the Warrants is most appropriate. As a result, the court denies their requests of limited intervention.

For the reasons stated above, it is this 9th day of November 2017, hereby

SO ORDERED.

Date: November 9, 2017

Chief Judge Robert E. Morin
Superior Court for the District of Columbia

Copies to:

Jennifer A. Kerkhoff
John W. Borchert
Assistant United States Attorneys

John Roche
Counsel for Facebook, Inc.

Scott Michelman
Arthur Spitzer
Shana Knizhnik
Counsel for the Account Holders

Paul Alan Levy
Counsel for Proposed Interveners