UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**No. 21-cr-332-PLF-1**
	:	
PAUL RUSSELL JOHNSON	:	
	:	
and	:	
	:	
STEPHEN CHASE RANDOLPH,	:	
	:	
Defendants.	:	

GOVERNMENT'S OPPOSITION TO DEFENDANT PAUL RUSSELL JOHNSON'S MOTION TO SUPPRESS ELECTRONIC EVIDENCE OR, IN THE ALTERNATIVE, TO APPOINT A SPECIAL MASTER

The United States hereby files this opposition to defendant Paul Russell Johnson's "Motion to Suppress Electronic Evidence Or, in the Alternative, to Appoint a Special Master." ECF No. 57 (hereinafter, "Motion"). For the reasons set forth below, the Court should deny the suppression motion in its entirety, and should further deny the defendant's request to appoint a special master to review and segregate documents and communications that are potentially protected by attorney-client privilege or the work product doctrine.

BACKGROUND

I. Summary of Relevant Facts

Defendant Paul Russell Johnson ("Johnson") is charged with, among other felonies, assaulting U.S. Capitol Police ("USCP") Officer C.E. with a deadly or dangerous weapon and inflicting bodily injury.

On January 6, 2021, at approximately 12:45 p.m., the defendant joined a group of rioters gathered at the Peace Circle, on the northwest side of the Capitol grounds. By the time the

defendant arrived at the Peace Circle, USCP officers had erected several rows of metal pedestrian barricades to block the pathway leading form the Peace Circle to the Lower West Terrace of the U.S. Capitol Building. Affixed to the pedestrian barricades were large white signs with the words "AREA CLOSED" in bold red lettering. Ignoring those signs, the defendant and other rioters moved past the first line of barricades and toward a second line of barricades further up the walkway. Several USCP officers were guarding the second line of barricades. When the defendant and other rioters approached the second line of barricades, they began verbally harassing the officers. They then began to violently lift and shove the metal barricades into the USCP officers, which caused Officer C.E. to fall backward, hit the stairs behind her, and suffer a concussion. The remainder of USCP officers were forced to retreat as scores of rioters began to trample over the fallen metal barricades—barricades that the defendant had personally helped level to the ground.

The defendant opened the floodgates to the January 6 riot. What followed were hours of terror, violence, and destruction as thousands of rioters made their way onto the Capitol grounds and inside the U.S. Capitol Building.[1]

On April 12, 2021, the United States District Court for the District of Columbia issued an arrest warrant based on a complaint charging the defendant with one felony count of Assaulting, Resisting, or Impeding Certain Officers and Inflicting Bodily Injury, in violation of 18 U.S.C. § 111(a)(1) and (b); one felony count of Obstructing Law Enforcement During Civil Disorder, in violation of 18 U.S.C. § 231(a)(3), one felony count of Obstruction of an Official Proceeding, in violation of 18 U.S.C. §§ 1512(c)(2) and 2; Engaging in Physical Violence in a Restricted Building

[1] A more fulsome description of the defendant's offense conduct is provided in the Government's Opposition to Defendant Paul Russell Johnson's Motion to Modify Conditions of Release. ECF No. 34, at 3-8.

or Grounds, in violation of 18 U.S.C. § 1752(a)(4); and Engaging in an Act of Physical Violence in the Capitol Grounds or Buildings, in violation of 40 U.S.C. § 5104(e)(2)(F). ECF No. 1.

Also on April 12, 2021, the United States District Court for the Eastern District of Virginia issued a search warrant authorizing the government to search: (1) Johnson's person; (2) Person-1's[2] person; (3) Johnson's residence; (4) mobile devices in Johnson's possession; and (5) mobile devices in Person-1's possession, for fruits, evidence, information, contraband, or instrumentalities of the following target offenses: 18 U.S.C. § 111(a)(1) and (b); 18 U.S.C. § 231; 18 U.S.C. §§ 1512(c)(2) and 2; 18 U.S.C. § 1752(a)(1), (2), and (4); and 40 U.S.C. § 5104(e)(2)(D), (F), and (G) (hereinafter, the "Target Offenses"). *See* Motion, Exh. 2, Affidavit ¶¶ 3-5.

Attachment A of the Affidavit in Support of the Search Warrant specifically describes the devices to be searched as "mobile phones in the possession of P. JOHNSON and [Person-1] or mobile devices located at the SUBJECT RESIDENCE available for use by P. JOHNSON or [Person-1]." Motion, Exh. 2, Att. A, at 53.[3] Attachment B of the Affidavit specifically lists, among the items to be seized, the "Subject Devices, as described in the Affidavit and Attachment A," as well as "[e]vidence of communication devices, including closed circuit radios or walkie-talkies, that could have been used by co-conspirators to communicate during the unlawful entry into the U.S. Capitol," and "[r]ecords and information—including but not limited to . . . photographs [and] videos . . . relating to . . . the Subjects' presence at the January 6, 2021, riot . . .

[2] Because this individual has not been charged, the government will refer to him/her as "Person-1" to protect his/her reputational and privacy interests and due process rights. For this reason, the parties have also redacted references to Person-1 from the Search Warrant Affidavit, which is Exhibit 2 to the defendant's Motion.

[3] Hereinafter, the pincites for Attachments A and B correspond to the page numbers at the bottom of these attachments.

[and] [t]he Subjects' (and other's) activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 6, 2021." *Id.*, Att. B, at 55-56.

Attachment B of the Affidavit also sets forth detailed filter protocols that the government will employ if the government identifies seized materials that are potentially privileged. Specifically, Attachment B provides that:

> If the government identifies seized materials that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e. communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.

Id. at 58-59.

At 6:00 a.m. on April 13, 2021, a team of 23 law enforcement officers executed the search warrant at the defendant's 14-acre property in the Eastern District of Virginia.[4] Motion, Exh. 3,

[4] Insofar as the defendant attempts to challenge the manner in which the search warrant was executed, the defendant may do so only by filing a civil Section 1983 lawsuit, not a motion to suppress. *See, e.g.*, Motion, at 3 (accusing law enforcement of showing an unreasonable amount of force to search and seize a man). The defendant's unsolicited thoughts about how the arrest and search warrant could have been executed are, first and foremost, irrelevant, and second, uninformed. The defendant blithely ignores the officer safety considerations that would have dictated the FBI's operational plan. After all, the defendant was known to possess several firearms, the defendant resides on a 14-acre property with several unknown structures, and the defendant is charged with assaulting a law enforcement officer and causing the officer to suffer bodily injury at the Capitol on January 6, 2021. Such factors amply justify the use of a SWAT team to execute the arrest and search warrants in this case.

at 1-2. During the search, law enforcement seized twenty items, including, as relevant here, the following devices:

(1) One Black Motorola phone;

(2) One Samsung phone;

(3) Two Explore One HD Cameras

(4) Four walkie-talkies; and

(5) One black Lenovo IdeaCentre desktop computer.

Motion, Exh. 1, at 2-3, Exh. 3, at 4. Law enforcement did not seize Person-1's cell phone. Instead, law enforcement imaged Person-1's cell phone onsite and returned the cell phone to Person-1 the same day. Law enforcement also manually searched through Johnson's son's cell phone, but did not seize any content from the cell phone. Law enforcement ultimately returned the son's cell phone to Person-1 on April 13. Motion, Exh. 3, at 3-4.

II. Procedural History

The defendant was arrested on April 13, 2021, and had his initial appearance in the Eastern District of Virginia on April 14, 2021. On April 29, 2021, the defendant had his initial appearance before Magistrate Judge Harvey in the District of Columbia. ECF No. 20.

On April 30, 2021, a federal grand jury in the District of Columbia returned a nine-count indictment charging Johnson and co-defendant Stephen Chase Randolph ("Randolph") with Obstruction of Law Enforcement During a Civil Disorder, in violation of 18 U.S.C. § 231(a)(3) (Count 1); Obstruction of an Official Proceeding and Aiding and Abetting, in violation of 18 U.S.C. §§ 1512(c)(2) and 2 (Count 2); Assaulting, Resisting, or Impeding Certain Officers Using a Dangerous Weapon, Inflicting Bodily Injury, and Aiding and Abetting, in violation of 18 U.S.C. §§ 111(a)(1), (b), and 2 (Count 3); three felony counts relating to disorderly conduct and violence

in a restricted building or grounds with a deadly or dangerous weapon, in violation of 18 U.S.C. § 1752 (Counts 5-7); and two misdemeanor counts relating to disorderly conduct and violence in a Capitol building or grounds, in violation of 40 U.S.C. § 5104(e)(2) (Counts 8-9). ECF No. 15. Randolph was charged alone in a separate count with Assaulting, Resisting, or Impeding Certain Officers, in violation of 18 U.S.C. § 111(a)(1) (Count 4). *Id.*

On July 16, 2021, the defendant filed a motion to modify his conditions of pretrial release in order to remove the home detention requirement and discontinue location monitoring. ECF No. 33. The Court orally denied this motion at the hearing on July 29, 2021.

On September 23, 2021, the defendant filed a motion to sever his case from that of co-defendant Randolph's. ECF No. 43. A hearing on this motion was held on October 19, 2021. The Court held the defendant's motion to sever in abeyance pending further discussions between the parties.

On November 19, 2021, the defendant filed the instant motion to suppress. The defendant does not challenge the entirety of the search warrant, thus conceding that there was probable cause to believe that the defendant committed federal crimes, and that there would be evidence of those crimes on his person, in his residence, and on his cell phones. Rather, the defendant's motion is limited to three arguments. First, the defendant argues that the government illegally seized the Lenovo IdeaCentre desktop computer, two Explore One HD cameras, and four walkie-talkies from his residence. Motion, at 8-9. Second, the defendant contends that the search warrant is unconstitutionally overbroad because it fails to set forth specific protocols for searching cell phones. *Id.* at 10-14. Finally, the defendant argues that even if the search warrant is not unconstitutionally overbroad and the government is permitted to search the cell phones and other electronic devices, the Court should appoint a special master to review the electronic evidence for

potentially privileged materials. *Id.* at 15-17. Each of these arguments is without merit, and the defendant's Motion should be dismissed in its entirety.

ARGUMENT

I. Johnson's Motion to Suppress Evidence from the Lenovo IdeaCentre Desktop Computer is Moot Because the Government Does Not Intend to Introduce Evidence Seized from this Device at Trial.

While the government maintains that it had probable cause to search the Lenovo IdeaCentre desktop computer seized from Johnson's residence, the government will not seek to introduce any evidence from this device at trial. Accordingly, the Court should deny as moot the motion to suppress with respect to the Lenovo IdeaCentre desktop computer. *See, e.g.*, *United States v. Jones*, 142 F. Supp. 3d 49, 54 n.2 (denying as moot a defendant's motion to suppress statements where the government represented that it will not seek to introduce any of those statements).

II. Law Enforcement Had Probable Cause to Seize the Explore One HD Cameras, and Relied in Good Faith on the Search Warrant to Seize the Four Walkie-Talkies.

The defendant contends that the government lacked probable cause to seize the two Explore One HD cameras and four walkie-talkies because the Affidavit "provided no reason to believe that Mr. Johnson possessed any of these devices or that they would be found in his home." Motion, at 9. The defendant is incorrect. The search warrant sets forth probable cause to seize the Explore One HD cameras, and officers relied in good faith on the search warrant—which specifically authorized the seizure of walkie-talkies and other communication devices—to seize the walkie-talkies.

A. Applicable Law

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause." U.S. Const. amend. IV. To comply with that requirement, the affidavit in support of a request for a warrant must provide a "'substantial basis for concluding that probable cause

existed.'" *United States v. Warren,* 42 F.3d 647, 652 (D.C. Cir. 1994) (quoting *Illinois v. Gates,* 462 U.S. 213, 238-39 (1983)). "'In dealing with probable cause, . . . as the very name implies, [courts] deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Gates*, 462 U.S. at 231 (quoting *Brinegar v. United States*, 338 U.S. 160, 175 (1949)). "The task of a judge reviewing an affidavit for probable cause 'is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Washington,* 775 F.3d 405, 407 (D.C. Cir. 2014) (quoting *Gates,* 462 U.S. at 238).

The issuing judge's "'determination of probable cause should be paid great deference by reviewing courts.'" *Gates*, 462 U.S. at 236 (quoting *Spinelli v. United States*, 393 U.S. 410, 419 (1969)); *see also United States v. Webb,* 255 F.3d 890, 904 (D.C. Cir. 2001). "[T]he traditional standard for [a] review of an issuing magistrate's probable cause determination has been that so long as the magistrate had a 'substantial basis for . . . conclud[ing]' that a search would uncover evidence of wrongdoing, the Fourth Amendment requires no more." *Gates*, 462 U.S. at 236 (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)).

Probable cause to search a residence exists when "there is a fair probability that contraband or evidence of a crime will be found in a particular place," *Gates*, 462 U.S. at 238. Moreover, "'[t]here must, of course, be a nexus . . . between the item to be seized and criminal behavior.'" *United States v. Griffith*, 867 F.3d 1265, 1271 (D.C. Cir. 2017) (citing *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967)). "[T]he nexus between the objects to be seized and the premises searched can be established from the particular circumstances involved and need not

rest on direct observation." *United States v. Lockett,* 674 F.2d 843, 846 (11th Cir. 1982). "A magistrate may infer a nexus between a suspect and [evidence in] his residence, depending upon the type of crime being investigated, the nature of things to be seized, the extent of an opportunity to conceal the evidence elsewhere and the normal inferences that may be drawn as to likely hiding places." *United States v. Williams,* 544 F.3d 683, 687 (6th Cir. 2008) (internal quotation marks and citation omitted); *see United States v. Hodge*, 246 F.3d 301, 305-06 (3d Cir. 2001) (noting that a court "is entitled to draw reasonable inferences about where evidence is likely to be kept, based on the nature of the evidence and the type of offense" (internal quotation marks and citation omitted)).

In sum, to pass constitutional muster, a search warrant affidavit must establish probable cause to believe that a crime was committed and that the premises to be searched contain the evidence, fruits, or instrumentalities of criminal activity. The warrant itself must also contain a "description of the objects to be seized" that is no "broader than can be justified by the probable cause upon which the warrant is based." *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013) (quoting 2 W. LaFave, *Search and Seizure* § 4.6(a) (5th ed. 2012)).

Even if a reviewing court disagrees with the magistrate's finding of probable cause, such disagreement does not automatically suggest the need to suppress evidence uncovered during the search. In *United States v. Leon,* the Supreme Court confirmed a "good faith" exception to the exclusionary rule. 468 U.S. 897 (1984). There, the Court held that law enforcement officers may rely on the probable cause determination of the magistrate approving the search warrant in conducting the search. *Id.* at 922. As long as the executing officer relied in good faith on the warrant, the exclusionary rule does not apply. *Id.* at 920.

The Court in *Leon* did, however, identify four situations in which it is not appropriate to apply the "good faith" exception because the officer "will have no reasonable grounds for believe that the warrant was properly issued." *Id.*at 923. Those situations were:

> (1) where the magistrate issued the warrant based on a deliberately or recklessly false affidavit; (2) where the issuing magistrate failed to act in a neutral and detached manner; (3) where a warrant is based on an affidavit "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and (4) where a warrant is "so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid."

United States v. Johnson, 332 F. Supp. 2d 35, 38-39 (D.D.C. 2004) (quoting *Leon*, 468 U.S. at 923). Overall, however, as the Court in *Leon* explained, "[w]hen officers have acted pursuant to a warrant, the prosecution should ordinarily be able to establish objective good faith without a substantial expenditure of judicial time." *Id.* at 924.

B. Analysis

1. There Was Probable Cause to Seize the Explore One HD Cameras.

Attachment A of the Affidavit specifically defines "Subject Devices" to include "mobile devices." Motion, Exh. 2, Att. A, at 53. As evident from the photograph below (which was taken during the search at Johnson's residence on April 13, 2021), the Explore One HD camera is a mobile device.[5]

[5] According to an Amazon.com description, the Explore One HD Camera is capable of being worn or mounted on a selfie stick, a tripod, or a pole mount. *See* ExploreOne 1080P HD Action Camera with Wi-Fi Item 245002," Amazon.com, *available at* amazon.com/ExploreOne-1080P-Action-Camera-2450002/dp/B08GX89GRY (last accessed Dec. 3, 2021). It is therefore "mobile," as that term is ordinarily understood.

In addition to being a mobile device, the Explore One HD camera can also contain "[r]ecords and information—including but not limited to . . . photographs [and] videos . . . relating to . . . "the Subjects' presence at the January 6, 2021, riot riot . . . [and] [t]he Subjects' (and other's) activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 6, 2021," and can therefore be seized under paragraph 3 of Attachment B of the search warrant. *Id.* at 55-56. Indeed, while several paragraphs in Attachment B specifically cross-reference the term "Subject Devices" from Attachment A, paragraph 3 of Attachment B does not. Yet paragraph 3 of Attachment B clearly contemplates the seizure of electronic devices, since it authorizes the seizure of records and information in the format of "emails" and "online postings," which would likely only be available in digital format. Motion, Exh. 2, Att. B, at 55-56. Moreover, the Affidavit establishes probable cause to search other digital devices (beyond just mobile phones) based on the representation that "[i]nformation from wireless telephones may also be saved or backed up on computers, mobile storage devices, or other electronic devices; and those other electronic devices may contain independently derived evidence, fruits, and instrumentalities of the crime in question." Motion, Exh. 2, Affidavit ¶ 76.

The Affidavit also establishes probable cause to believe that the defendant possessed or used a mobile device like a camera to record his activities on January 6, 2021. Specifically,

paragraphs 54 and 74 of the Affidavit describe a YouTube video in which the defendant can be heard saying to another individual, "I have video where I'm slinging one around." Affidavit ¶¶ 54, 74. This video of the defendant "slinging one around" could reasonably have been recorded and stored on other devices beyond just the defendant's cell phone. Paragraph 76 of the Affidavit further provides that "[i]nformation from wireless telephones may also be saved or backed up on computers, mobile storage devices, or other electronic devices; and those other electronic devices may contain independent derived evidence, fruits, and instrumentalities of the crime in question." *Id.* ¶ 76. It is reasonable to believe that such "mobile storage devices" and "electronic devices" could include the Explore One HD cameras seized from the residence, and that such devices would contain evidence of the identified offenses.

Finally, the Affidavit establishes that there was a fair probability that mobile devices, like cameras, would be located at the defendant's residence. Specifically, paragraph 71 sets forth probable cause to believe that the cameras, along with other digital devices, would be stored at the defendant's residence: "I know, based on my training and experience, that people who spend time at a particular address also store their belongings and devices as part of their daily lives at that address." *Id.* ¶ 71. Accordingly, there was probable cause to seize and to search the Explore One HD cameras for the items listed in Attachment B.

2. Officers Relied in Good Faith on Attachment B of the Search Warrant to Seize the Walkie-Talkies.

Even assuming, *arguendo*, that the Affidavit lacked probable cause to seize the walkie-talkies, the Court should deny the defendant's motion to suppress these devices based on the *Leon* good-faith exception. Attachment B of the search warrant specifically authorized the seizure of "communication devices, including closed circuit radios or *walkie-talkies*, that could have been used by co-conspirators to communicate during the unlawful entry into the U.S. Capitol." Motion,

Exh. 2, Att. B ¶ 1(k) (emphasis added). Accordingly, the good faith exception applies to law enforcement's seizure of these devices.

The only potentially applicable exception to the *Leon* good-faith exception in this case would be the third exception—that is, whether the search warrant was based on an affidavit "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Id.* The defendant does not make this argument, nor could he prevail on this argument in any event.

The cases granting motions to suppress on the basis of the third exception to *Leon* "appear to include situations where, for example, the affidavit failed to link the suspect to the location to be searched . . . failed to explain why the affiant believed evidence of criminal activity would be found at the location, [and] failed to explain why evidence would be present long after officers received relevant information to support the affidavit." *United States v. Savoy*, 889 F. Supp. 2d 78, 90 (D.C. Cir. 2012). That is not the situation here. The Affidavit describes in significant detail the investigative steps undertaken by law enforcement to confirm the defendant's residence, including checking property records for the residence, conducting surveillance at the residence, observing vehicles registered to the defendant parked at the residence, and observing the defendant personally exit the residence. Motion, Exh. 2, Affidavit ¶¶ 66-70. The Affidavit also explains why the affiant believed evidence of criminal activity would be found at the location. For example, paragraph 71 of the Affidavit describes why the affiant believed that the residence was likely to contain clothing and accessories consistent with what the defendant was seen wearing on January 6, 2021. *Id.* ¶ 71. Paragraph 72 of the Affidavit describes why the affiant believed that the residence was likely to contain evidence of the defendant's motive, planning, coordination, intent, and travel to Washington D.C. *Id.* ¶ 72. Moreover, only three months had elapsed between the

defendant's participation in the January 6 riot and the search of his residence; accordingly, it was reasonable for the affiant to believe that evidence of criminal activity would be present at the residence.

In sum, because the search warrant was replete with indicia of probable cause, it was objectively reasonable for agents to rely on paragraph 1(k) of Attachment B when seizing the walkie-talkies. The *Leon* good faith exception applies, and the defendant's motion to suppress the walkie-talkies should be denied.

III. The Defendant Has Not Established Standing to Contest the Seizure and Search of Person-1's Cell Phone or His Son's Cell Phone.

The defendant claims he has standing to challenge the search of Person-1's cell phone and his son's cell phone because the contents of those phones "are all backed up on a cloud computing service, and the account for all of the cell phones is in Mr. Johnson's name." Motion at 6. This unsworn assertion falls woefully short of satisfying the defendant's burden of establishing a legitimate, subjective expectation of privacy in these cell phones.

A. Applicable Law

1. Standing to Contest a Search Warrant.

It is well established that a defendant has no right to have evidence suppressed on Fourth Amendment grounds unless he demonstrates that he had a "legitimate expectation of privacy" in the area searched. *Rakas v. Illinois*, 439 U.S. 128, 143 (1978); *see also Rawlings v. Kentucky*, 448 U.S. 98, 104-05 (1980)).

A showing of standing is required under the law because a "person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed." *Rakas*, 439 U.S. at 134. Absent such a showing, the defendant lacks standing to

challenge the search; therefore, the remedy provided by the exclusionary rule is unavailable. *See id.*; *Rawlings*, 448 U.S. at 100.

This standing requirement applies equally to searches of cell phones—where the defendant must establish ownership or another possessory interest in the phone at the time for which the data is searched—as it does to searches of physical premises. *See, e.g.*, *United States v. Dore*, 586 F. App'x 42, 46 (2d Cir. 2014) (denying a cell site challenge, holding that the defendant "does not have standing to assert Fourth Amendment rights in those phone records" because "he did not submit an affidavit establishing that the cell phones in question belonged to him or that he had a subjective expectation of privacy in them").

2. The Burden of Establishing Standing and a Reasonable Expectation of Privacy Falls Squarely on the Defendant.

The defendant bears the burden of establishing that he had a reasonable expectation of privacy in the phones seized and searched. The defendant must establish: (1) an actualsubjective expectation of privacy with respect to the place being searched or items being searched; and (2) that the defendant's subjective expectation of privacy is one that society is prepared to recognize as reasonable. *Smith v. Maryland*, 442 U.S. 735, 740-41 (1979); *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

Courts have identified several factors to be considered in determining whether there exists a reasonable expectation of privacy:

> whether the defendant has a property or possessory interest in the thing seized or the place searched, whether he has a right to exclude others from that place [or the thing seized], whether he has exhibited a subjective expectation of privacy that it would remain free from governmental intrusion, whether he took normal precautions to maintain privacy, and whether he was legitimately on the premises [or legitimately in possession of the thing seized].

United States v. Finley, 477 F.3d 250, 258-59 (5th Cir. 2007) (quoting *United States v. Cardoza-Hinojosa*, 140 F.3d 610, 615 (5th Cir. 1998)) (original alterations and quotation marks omitted); *United States v. Lopez-Cruz*, 730 F.3d 803, 808 (9th Cir. 2013) (same); *United States v. Burnett*, 890 F.2d 1233, 1237 (D.C. Cir. 1989) (same).

As many courts have held, in order to establish an actual, subjective expectation of privacy in the item being searched, the defendant "must submit an affidavit from someone with personal knowledge demonstrating sufficient facts to show that he had a legally cognizable privacy interest in the searched premises at the time of the search." *United States v. Ruggiero*, 824 F. Supp. 379, 391 (S.D.N.Y. 1993); *United States v. Montoya-Eschevarria*, 892 F. Supp. 104, 106 (S.D.N.Y. 1995) ("The law is clear that the burden on the defendant to establish standing is met only by sworn evidence, in the form of affidavit or testimony, from the defendant or someone with personal knowledge."); *see also United States v. Hamlett*, Case No. 3:18-cr-24 (VAB), 2018 WL 4656241, at *5 (D. Conn. Sept. 27, 2018) (finding no standing where defendant did not "offer any testimony to establish that he had an ownership or cognizable property interest in the cellphone at issue").

B. Analysis

Here, the defendant has submitted no sworn evidence establishing his subjective expectation of privacy in Person-1's cell phone or in his son's cell phone. He has therefore failed to satisfy his burden of establishing a subjective expectation of privacy in either device.

Even if this Court were to credit defense counsel's unsworn assertion that Person-1's and Johnson's son's cell phones are backed up to a cloud computing service in Johnson's name, this does not establish Johnson's subjective expectation of privacy in the physical devices. The defendant's alleged ownership of the cloud computing account would potentially be relevant if the

government were searching the cloud account. But here, the defendant has made no attempt to show that he exhibited a subjective expectation of privacy in the physical devices.

Any argument that the defendant had some type of property interest in Person-1's and his son's cell phone should also fail, because a mere property interest is insufficient to establish a subjective and reasonable expectation of privacy. *Cf. Finley*, 477 F.3d at 258-59 (holding that an employee had a reasonable expectation of privacy in a business phone issued to him by his uncle's business because the employee maintained a property interest in the phone, had a right to exclude others from using the phone, exhibited a subjective expectation of privacy in the phone, and took normal precautions to maintain his privacy in the phone, and further noting that a property interest in the item searched is only one factor in the analysis and is not dispositive).

Finally, insofar as the defendant challenges the search of his son's cell phone, Attachment A of the search warrant specifically provides for the search of "mobile devices located at the SUBJECT RESIDENCE available for use by P. JOHNSON and [Person-1]." Exh. 2, Att. A, at 53. Johnson's son's cell phone plainly qualifies as a subject device under Attachment A, since it was located at the residence and was available for use by anyone, not just Johnson's son. Moreover, the defendant's motion is moot with respect to the search of the son's cell phone because the government did not seize evidence from this device and will not be introducing any evidence from this device at trial.

IV. The Search Warrant Describes with Sufficient Particularity the Items to be Seized from Johnson's Cell Phones and is Not Overbroad.

While Johnson does not dispute that there was probable cause to seize his cell phones, he contends that the search warrant is unconstitutionally overbroad because it does not "articulate with sufficient particularity the data and information to be searched and seized on the electronic devices." Motion at 10. Relying on *Riley v. California*, 573 U.S. 373 (2014), the defendant

suggests that "probable cause is required to search each of the different types of data and other information stored on a cell phone." Motion at 10.

Riley is inapposite. *Riley* involved only the question of whether probable cause is required to conduct a search of cellphone data. It did not address the question of whether, as here, after law enforcement has made a showing that there is probable cause that a federal crime has been committed and has established probable cause that the cell phone will contain evidence of the identified offenses, an issuing magistrate is still required to limit the communications that law enforcement can seize to those that law enforcement has already identified, and cannot give law enforcement authority to seize the communications of which it is not yet aware but nonetheless constituted evidence of the crime.

As detailed below, a vast majority of federal courts have rejected similar particularity challenges to search warrants for digital devices. This Court should too.

A. Applicable Law

1. Particularity.

The Fourth Amendment requires that warrants "particularly describe[e]" the "things to be seized." U.S. Const. amend. IV. That condition "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." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

When assessing whether a warrant is sufficiently particular, courts "'are concerned with the realities of administration of criminal justice. It is sufficient if the warrant signed by the judicial officer is particular enough if read with reasonable effort by the officer executing the warrant.'" *United States v. Vaughn*, 830 F.2d 1185, 1186 (D.C. Cir. 1987) (quoting *Moore v. United States*, 461 F.2d 1236, 1238 (D.C. Cir. 1972)) (internal quotation marks omitted). Generally, a warrant

will satisfy the particularity requirement when it allows police officers "'to seize only evidence of a particular crime.'" *United States v. Manafort*, 313 F. Supp. 3d 213, 232 (D.D.C. 2018) (quoting *United States v. Young*, 260 F. Supp. 3d 530, 546 (E.D. Va. 2017)).

Courts "may 'consider [] the circumstances of the crime in assessing the degree of particularity that should be required of descriptions of items to be seized in the warrant.'" *Manafort*, 313 F. Supp. 3d at 233 (quoting *United States v. Dale*, 991 F.2d 819, 848 (D.C. Cir. 1993) (per curiam)). Overall, "[t]he Fourth Amendment does not require a perfect description of the data to be searched and seized," and "[s]earch warrants covering digital data may contain 'some ambiguity . . . .'" *United States v. Ulbricht*, 858 F.3d 71, 100 (2d Cir. 2017) (quoting *Galpin*, 720 F.3d at 446).

2. Failure to Include Phone-Specific Search Protocols Does Not Render a Search Warrant Unconstitutionally Overbroad.

"'Nothing in the language of the Constitution or in th[e] [Supreme] Court's decisions interpreting that language suggests that, in addition to the requirements set forth in the text [of the Fourth Amendment], search warrants also must include a specification of the precise manner in which they are to be executed." *United States v. Gubbs*, 547 U.S. 90, 97–98 (2006) (quoting *Dalia v. United States*, 441 U.S. 238, 255 (1979). Unsurprisingly, then, in the context of searches of digital devices, such specificity is routinely held not to be required. *See, e.g.*, *United States v. Richards*, 659 F.3d 527, 538 (6th Cir. 2011) ("[G]iven the unique problem encountered in computer searches, and the practical difficulties inherent in implementing universal search methodologies, the majority of federal courts have eschewed the use of a specific search protocol and, instead, have employed the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis.") (citations omitted); *id.* at 538 n.9 (collecting cases).

There are also several impracticalities to including limitations on the scope and mechanics of a search of electronic information. To prospectively restrict the scope of a search by filename or application would "unduly restrict legitimate search objectives," *United States v. Burgess*, 576 F.3d 1078, 1093-94 (10th Cir. 2009), and "would give criminals the ability to evade law enforcement scrutiny simply by utilizing coded terms in their files or documents, or placing such documents in areas of the computer that would not normally contain such files/documents," *United States v. Graziano*, 558 F. Supp. 2d 304, 315 (E.D.N.Y. 2008). *See also* Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 545 (2005) ("Exact search protocols are difficult to settle ex ante; good forensic analysis is an art more than a science."). As the Second Circuit has observed, "it will often be impossible to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes." *Ulbricht*, 858 F.3d at 102. Moreover, "[f]iles and documents can easily be given misleading or coded names, and words that might be expected to occur in pertinent documents can be encrypted; even very simple codes can defeat a pre-planned word search." *Id.*

Finally, the Fourth Amendment does not prohibit law enforcement from seizing, pursuant to a warrant, electronic devices that are likely to contain evidence of crimes simply because that evidence is likely intermingled with other non-criminal and private information. "[T]raditional searches for paper records, like searches for electronic records, have always entailed the exposure of records that are not the objects of the search to at least superficial examination in order to identify and seize those records that are." *Id.* at 100. "And in many cases, the volume of records properly subject to seizure because of their evidentiary value may be vast." *Id.* But "[n]one of these consequences necessarily turns a search warrant into a prohibited general warrant." *Id.*

B. Analysis

Here, the search warrant provides meaningful parameters on the permissible search of the seized cell phones, and identifies with particularity the underlying information to be seized. The warrant does not permit the agents to take whatever they want from the cell phones regardless of its relevance to the Target Offenses. Rather, the Affidavit contains a representation that agents would extract and seize only "the information, records, or evidence described in Attachment B." Motion, Exh. 2, Affidavit ¶ 82(a). Exhibit B, in turn, sets forth narrow categories of evidence that are responsive to the warrant and that constitute fruits, evidence, information, contraband, or instrumentalities relating to violations of the Target Offenses. For example, Exhibit B limits the information permitted to be seized to specific time periods and specific types of records, such as records relating to the defendant's "presence at the January 6, 2021 riot," his "travel to or from Washington D.C. from December of 2020 through January of 2021," his "motive and intent for traveling to the U.S. Capitol on or about January 6, 2021," and his "activities in and around Washington D.C., specifically the U.S. Capitol, on or about January 6, 2021." Motion, Exh. 2, Att. B, at 54-56. Accordingly, the Court should dismiss the defendant's motion to dismiss the search warrant as unconstitutionally overbroad.

V. The Filter Procedures Set Forth in the Warrant Adequately Protect the Defendant's Privileged Communications.

The defendant contends, without any supporting authority, that this Court should appoint a special master to review the electronic evidence and separate out any potentially privileged materials. Motion, at 15-17. The government's filter protocols, as set forth in Attachment B of the search warrant, scrupulously protect the defendant's attorney-client privilege. Exh. 2, Att. B,

at 58-59. Moreover, the appointment of a special master to review the seized electronic devices is neither legally mandated nor warranted in this case.[6]

A. Applicable Law

Filter teams are routinely used as a method to safeguard parties' privileged documents without needlessly hindering an ongoing investigation or requiring *in camera* review of countless documents. *See, e.g.*, *In re Search Warrants Executed on Apr. 28, 2021*, Case No. 21-MC-425 (JPO), 2021 WL 2188150, at *2 (S.D.N.Y. May 28, 2021) (rejecting Rudolph Giuliani's objections to proposed filter team and acknowledging that "[t]he use of a filter team is a common procedure in this District and has been deemed adequate in numerous cases to protect attorney-client communications"). *See also United States v. Coffman*, 574 F. App'x 541, 564-65 (6th Cir. 2014); *United States v. Feng Ling Liu*, Case No. 12 Cr. 934(RA), 2014 WL 101672, at *12 (S.D.N.Y. Jan. 10, 2014); *United States v. SDI Future Health, Inc.*, 464 F. Supp. 2d 1027, 1037-38 (D. Nev. 2006); *In re Search of 5444 Westheimer Road Suite 1570*, Misc. Action No. H-06-238, 2006 WL 1881370, at *2 (S.D. Tex. July 6, 2006).

In assessing whether the use of a government filter team is a proper, fair, and acceptable method of protecting privileged communications, courts in this district have considered several factors, including: (1) whether government officials have already obtained the physical control of potentially privileged documents, (2) whether the lawfulness of the acquisition of the documents to be reviewed was initially challenged; (3) whether the materials for review are voluminous; and

[6] Agents had already begun searching the seized cell phones before defense counsel alerted the government in July 2021 that the seized devices may contain privileged materials on them. Upon learning of defense counsel's concerns, government counsel instructed the agents to stop reviewing the seized items. In or around November 2021, the FBI instructed its agents to assure that digital items that had been seized had been properly scoped. In order to complete this task, agents went back into the cell phones to tag and formally extract the items that they intended to seize as falling within the scope of Attachment B of the search warrant.

(4) the filter team's effect on the appearance of fairness. *United States v. Jackson*, Crim. Action No. 07-0035 (RWR), 2007 WL 3230140, at *5 (D.D.C. 2007) (internal quotation marks and citations omitted).

B. Analysis

The government's use of a filter team is a proper, fair, and acceptable method of protecting privileged materials in this case. First, the government is already in possession of the defendant's potentially privileged documents, such that the use of the filter team to "sift the wheat from the chaff constitutes an action respectful of, rather than injurious to, the protection of privilege." *In re Grand Jury Subpoenas*, 454 F.3d 511, 522-23 (6th Cir. 2006). Second, the defendant—until now—has not challenged the lawfulness of the acquisition of the cell phones to be reviewed, which generally favors use of the filter team. Moreover, as the defendant concedes, there was probable cause to believe that he committed federal crimes, and that there would be evidence of those crimes on his cell phones. Third, as the defendant acknowledges, cell phones can contain vast quantities of information. *See* Motion, at 6-7. But special masters are "usually appointed when the materials for review 'are not voluminous,' and therefore are less useful in cases involving significant problems with time, manpower, and multiple languages." *Hicks v. Bush*, 452 F. Supp. 2d 88, 103 n.12 (D.D.C. 2006). Use of a special master would slow the pace of discovery and would negatively affect the defendant's ability to obtain a speedy trial—a right that he has emphatically asserted in this case. Finally, use of a filter team in this case does not affect the appearance of fairness. As defense counsel is aware, the government's proposed filter team is from a different United States Attorney's Office that is completely walled off from the District of Columbia. Moreover, as set forth in the filter protocols in Attachment B, the filter team does not have the unilateral authority to disclose potentially protected materials. Rather, if the filter team believes

that potentially protected materials are not protected (for example, because the communication includes a third party or the crime-fraud exception applies), the filter team must first obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these materials to the prosecution team. Motion, Exh. 2, Att. B, at 58-59.

The defendant cites only two authorities in support of his demand for the appointment of a special master: (1) the Department of Justice's Justice Manual; and (2) the Fourth Circuit's decision in *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159 (4th Cir. 2019). Neither authority supports defendant's argument that a special master is required in this case.

The Justice Manual, formerly known as the U.S. Attorney's Manual, "is not intended to, does, not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter, civil or criminal." *United States v. Blackley*, 986 F. Supp. 607, 613 (D.D.C. 1997) (citing *United States v. Busher*, 817 F.2d 1409, 1411-12 (9th Cir. 1987)); *see also* U.S. Justice Manual, § 1-1.200 (2018) (expressly providing that the Manual "is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal").

But even if it were appropriate to consider the Justice Manual—which it is not—the Justice Manual, by its own terms, does not prescribe the appointment of a special master in this case. To the contrary, the section of the Justice Manual cited by the defendant applies only to "Searches of Premises of Subject Attorneys," and actually endorses the use of a "'privilege team . . . consisting of agents and lawyers not involved in the underlying investigation," when searching subject attorneys' premises. *See* U.S. Justice Manual § 9-13.420. Moreover, as the defendant's motion concedes, DOJ's guidelines for reviewing computer files for privileged materials do not mandate the use of a special master. *See* Motion, at 16 n.2.

The Fourth Circuit's decision in *In re Search Warrant* is also inapposite. In that case, the Fourth Circuit found that a magistrate judge who authorized a warrant to search a law firm office erred by permitting a government filter team to review and provide to the prosecution, without the consent of the law firm or a court order, any documents it unilaterally found non-privileged. 942 F.3d at 166, 176. *In re Search Warrant* did not hold that the government's use of a filter team is categorically inappropriate. *See In re Search Warrants Executed on Apr. 28, 2021*, Case No. 21-MC-425 (JPO), 2021 WL 2188150, at *2 n.3 (S.D.N.Y. May 28, 2021).

Moreover, the facts and circumstances in that case—which one member of the panel stressed were "unique," *In re Search Warrant*, 942 F.3d at 183 (Rushing, J., concurring)—are very different from those here. In *In re Search Warrant*, the movant was a law firm that was itself under investigation for potentially conspiring with one of its clients to launder drug money. Approximately 99.8% of the 52,000 emails seized did not involve the client whose relationship with a member of the firm was under investigation; the firm involved did criminal defense work and "many" of the seized emails contained privileged information relating to *other* clients, some of whom were potential subjects or targets of investigations by the office conducting the review; the law firm immediately and vigorously objected to review of the seized materials by the filter team; if the filter team determined that a communication was not privileged, the law firm was not given an opportunity to object; and the filter team was prospectively authorized to contact clients of the firm *ex parte* to seek waivers of their attorney-client privileges. *Id* at 165-68.

None of these circumstances are present here. The defendant in this case is a professional tree cutter, not an attorney. By the defendant's own account, the privileged communications relate only to his family law proceedings in Virginia state court, and are not alleged to contain any attorney-client communications relating to the January 6 riot. *See* Motion, at 7, 15. This presents

a very different situation than filtering for privileged communications that relate to an ongoing government investigation or to a defendant's criminal case. First, there is less concern about the proverbial fox in the henhouse because the government has no interest in the privileged information. It's as if the fox were vegan. Second, the Court has no reason to be nervous about the government rummaging through and invading the defense camp, because none of the potentially privileged materials are said to contain any attorney-client communications regarding the instant criminal case. And third, the privileged information, as described by the defendant, likely would not fall within the scope of the warrant and would not, in any event, be seized.

Additionally, the filter protocols set forth in the search warrant are distinguishable from the filter protocols that raised concerns in *In re Search Warrant*. In *In re Search Warrant*, the "Privilege Assessment Provision" provided that when seized materials were found by the filter team to be nonprivileged, the filter team could forward such materials directly to the prosecution team without the consent of the law firm or a court order. 942 F.3d at 166. Here, by contrast, if ever the Filter Team concludes that potentially protected materials—that is, communications that are to/from an attorney, or that otherwise reference or reflect attorney advice—are not protected, the Filter Team cannot unilaterally act to disclose those materials to the Prosecution Team. Instead, the Filter Team must obtain "either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team." Motion, Exh. 2, Att. B, at 59. *See also In re Search Warrant*, 942 F.3d at 184 (Rushing, J., concurring) (noting that the majority opinion does not suggest that the Modified Privilege Assessment Provision, which provided that "no documents—including those the Filter Team considers nonprivileged—can be sent to the Prosecution Team without either the consent of the Law Firm or a court order" impermissible usurp[ed] a judicial function"). In sum, the use of a

Filter Team to review the defendant's devices for potentially privileged communications does not raise any of the concerns that motivated the Fourth Circuit's opinion in *In re Search Warrant*.

Finally, this Court should not countenance the defendant's concerns about the Filter Team's "lack of first-hand knowledge of [Mr. Johnson's] underlying family law cases" when the defendant has repeatedly rebuffed the government's efforts to gather precisely this type of information. Ironically, the defendant has disclosed more information about the nature of the privileged materials in his instant motion than he has in response to multiple government inquiries intended to guide the Filter Team's review of the defendant's devices and to ensure that the Filter Team is as scrupulous as possible when reviewing the defendant's devices. For example, on July 14, 2021, defense counsel declined to respond to the following questions from undersigned counsel regarding the nature, volume, and type of privileged materials contained on the defendant's devices:

(1) Which devices contain potentially privileged materials?

(2) What specific names, email accounts, social media accounts, messenger app accounts, domain names, or phone numbers may be associated with potentially privileged materials? In addition to counsel, this includes members of the legal defense team, *e.g.*, defense investigators, paralegals, and support staff. This may also include members of a Joint Defense Agreement or Common Interest Agreement and their respective staff.

(3) What date ranges are impacted for *any* potentially privileged communications?

(4) With respect to the Capitol Riot investigation:

   a. What date was this attorney first contacted?

b. What date was any other attorney first contacted in connection with this investigation?

During this communication, the government further clarified that it considered potentially privileged materials to include any legal representation, regardless of whether it appears to be related to this case, *e.g.*, legal representation related to a business, entity, divorce, or estate plan, or involving an entity that could claim a corporate privilege over the data. Defense counsel declined to provide any information in response to this request.

Again, on November 18, 2021, a representative from the government's Filter Team—who is not employed by the United States Attorney's Office in the District of Columbia and who is walled off from the prosecution team—communicated with defense counsel about the government's filter protocols. The Filter Team representative informed defense counsel that the government strives to be "overly inclusive" in its approach to filtering privileged materials, and explained that the Filter Team removes "any communications that are or may potentially be privileged regardless of the subject matter," including "any communications between counsel and client even if there would otherwise be a reason not to find that the privilege exists." As the Filter Team representative further clarified for defense counsel, "unless there is any reason to believe crime-fraud applies to your client's communications, we would, if asked, summarily remove any privileged, and or potentially privileged, communications from the data before it is release to the investigators and case AUSA."

When defense counsel followed up to inquire how the government knows that something is "work product" if it does not involve an attorney (*e.g.*, when an investigator, working with the client and an attorney, interviews a witness and then reports that interview back to the client via e-mail), the Filter Team representative responded by explaining that "[g]enerally, if we know all the

parties associated with the attorney, we simply filter everyone out which would include investigators. Neither the case agent nor the prosecuting AUSA knows who or what we have filtered out. It is walled off to them. So if you're hesitant to reveal the name of an investigator to the AUSA, you may in confidence reveal it to me and we'll filter the data accordingly. That information is not disclosed to the case agent or AUSA." The Filter Team representative further clarified that the filter team does not "act in a judicial capacity," and that "[i]f [the filter team] believe[s] communications fall within an exception and are relevant and material, I will discuss it with you. If we do not reach an agreement, we will litigate it under seal. Again, the case AUSA is walled off from any such litigation and would only be made aware of the substance of the materials upon the order of the court." Again, defense counsel declined to provide any further information to the government's Filter Team.

As one court in this district has observed, "[t]here is no reason to think that a special master would be any more successful than a filter team at identifying privileged documents bearing no obvious privilege markings." *Hicks v. Bush*, Civil Action No. 02-0299, 2006 WL 8427192, at *8 n.12. Accordingly, and for the reasons explained above, this Court should reject the defendant's unfounded request to appoint a special master to review the contents of the digital devices seized.

CONCLUSION

For the foregoing reasons, the Government respectfully submits that the Court should deny the defendant's Motion to Suppress Electronic Evidence Or, in the Alternative, to Appoint a Special Master.

Respectfully submitted,

MATTHEW M. GRAVES
United States Attorney
D.C. Bar No. 481052

/s/ Hava Mirell
HAVA MIRELL
Assistant United States Attorney, Detailee
CA Bar No. 311098
555 Fourth Street, N.W.
Washington, DC 20530
(213) 894-0717
Hava.Mirell@usdoj.gov

Certificate of Service

I hereby certify that on December 3, 2021, I caused a copy of the foregoing memorandum to be served on counsel of record via electronic filing.

/s/ Hava Mirell
HAVA MIRELL
Assistant United States Attorney