UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	**:**	
v.	**:**	**Case No. 21-cr-332-PLF-1**
PAUL RUSSELL JOHNSON *et al.*,	**:**	
Defendants.	**:**	

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

Paul Russell Johnson, through counsel, moves this Court pursuant to the Fourth Amendment, Federal Rules of Criminal Procedure 41(h) and 12(b)(3)(C), and the relevant case law to suppress certain electronic devices unlawfully seized from him on April 13, 2021 in the pre-dawn raid of his home. Should this Court not find that law enforcement violated the Fourth Amendment, then Mr. Johnson requests that this Court appoint a neutral special master—as opposed to his governmental adversary—to review the attorney-client-privileged and/or work-product-protected material on his electronic devices.

INTRODUCTION

Photo 1: Paul Johnson cooperating with law enforcement, while they raid his family and farm with military assault rifles and an armored vehicle.

Photo 2: Law enforcement pointing a laser-equipped, military assault rifle at Person-1, who was in the home with two eight-year-old children and one 13-year-old child, while Mr. Johnson cooperated.

On April 13, 2021, at approximately 6:00 a.m., no less than twenty-three law enforcement officers raided Mr. Johnson's family. The raid included the Special Weapons Attack Team of the Federal Bureau of Investigation ("FBI"). Law enforcement knew that Mr. Johnson was non-violent. They were aware of his lack of a criminal record. They had surveilled his house on March 23, 2021, and they spoke with Person-1 on the same date. On March 25, 2021, law enforcement surveilled Mr. Johnson's cars. On April 7, 2021, law enforcement again watched Mr. Johnson. Law enforcement knew or should have known that Mr. Johnson runs a tree cutting business in Williamsburg, Virginia—E&E Tree Services. Law enforcement knew or should have known that Mr. Johnson is a lawful gun owner. Law enforcement knew or should have known that

Mr. Johnson and Person-1 are the putative parents to three kids—one teenager and two below the age of 10 on the day of the pre-dawn raid.

Law enforcement suspected that Mr. Johnson was involved in a crowd that toppled a fence and injured a police officer during the Stop the Steal Rally in Washington, DC on January 6, 2021. Law enforcement knew that Mr. Johnson was one of thousands, who while at the Rally, *never entered the U.S. Capitol*. When the Rally became too unruly, Mr. Johnson left.

Yet, in the face of this knowledge, suspected involvement at the Rally, and the presumption of Mr. Johnson's innocent, law enforcement showed an unreasonable amount of force to search and seize a man, who has no proven history of unreasonable force. As law enforcement often does, they could have quietly arrested Mr. Johnson at his business or when they watched him driving his vehicles down the street to the local gas station. Instead, law enforcement deeply traumatized the kids and the parents of a family on April 13, 2021, with assault weapons and an armored vehicle.

That unreasonable pre-dawn raid is paradigmatic of the unreasonable search and seizure of Mr. Johnson's electronic devices. That excessive show of force of that pre-dawn raid is a metaphor for the overbreadth of the Search Warrant in this case. Thus, this Court should find the Search Warrant violates the Fourth Amendment.

Specifically, the Search Warrant did not authorize the seizure of certain electronic devices—a desktop computer, two digital cameras, and four walkie talkies. In seizing these electronic devices, the government's actions are unconstitutionally unreasonable. The Search Warrant is unconstitutionally overbroad with regard to the proposed search of the three seized cellular phones. Due to this Fourth Amendment violation, Mr. Johnson requests that the Court suppress all electronic device evidence seized pursuant to the April 12, 2021 Search Warrant. If, however, the Court concludes that government can conduct its proposed blanket search of his

electronic devices, Mr. Johnson urges the Court to appoint a special master to review and segregate materials protected by attorney-client privilege or the work product doctrine.

FACTUAL BACKGROUND

The April 12, 2021 Search Warrant

On April 12, 2021, the government sought a warrant in the United States District Court for the Eastern District of Virginia for the seizure and search of, among other things, mobile devices in the possession of Mr. Johnson, in the possession of Person-1 and at his residence in Lanexa, Virginia. Ex. 1 at 1. To the Search Warrant application, the government attached an Affidavit from an agent from the FBI attesting why she had probable cause to search Mr. Johnson, Person-1, their residence in Lanexa, Virginia, and their mobile devices. Ex. 2, Maldonado Aff. ¶ 3.

Both the Affidavit and Attachment A to the Affidavit sought to seize and search only the "[m]obile devices in the possession of P. JOHNSON and Person-1 (or hereinafter 'the SUBJECT DEVICES')." Ex. 2, Maldonado Aff. ¶ 3(d); *Id.* Attach. A ("The devices to be searched are 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). The Affidavit then details the records and information the government has probable cause to believe it will find in the Subject Devices, *i.e.*, Mr. Johnson's and Person-1 mobile phones. *See* Ex. 2, Maldonado Aff. ¶¶ 79–80. Attachment B generally describes the "items to be seized" as "including, but not limited to" several different categories of evidence. Ex. 2, Maldonado Aff., Attach. B(a)–(m)). Attachment B describes the evidence to be seized from the Subject Devices, including but not limited to: (1) "who used, owned, or controlled the SUBJECT DEVICES at the time the things described in the warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles,

email, email contacts, chat, instant messaging logs, photographs, and correspondence"; (2) "evidence of the times the SUBJECT DEVICES [were] used"; and (3) "records of information about the SUBJECT DEVICES' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or favorite web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses." Ex. 2, Maldonado Aff., Attach. B ¶ 4(a), (e), (i).

Attachment B also addresses the review of seized materials that are potentially protected by attorney-client privilege or work product doctrine. *Id.* at 58–59. It provides for the creation of a Filter Team that "will have no future involvement in the investigation of this matter" if potentially privileged or protected materials are identified. *Id.* at 58. The Filter Team would review the materials and "provide all communications that are not potentially protected materials to the Prosecution Team." *Id.* at 59. "If the Filter Team concludes that any of the potentially protected materials are not protected (*e.g.*, the communication includes a third party of the crime-fraud exception applies), the Filter Team must either obtain agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team." *Id*. It does not provide a procedure for challenging the designation of materials as not protected or not privileged, either before or after those materials are provided to the Prosecution Team.

The Government's Seizure of Mr. Johnson's Electronic Devices

The FBI and other law enforcement executed the Search Warrant in the early morning hours of April 13, 2021. The FBI agents seized electronic devices including a Motorola cell phone, and Samsung cell phone, a Lenovo desktop computer, four walkie-talkies, and two Explore One HD cameras. Ex. 1 at 2–3; Ex. 3. The FBI agents also seized and imaged Person-1 cell phone. The FBI agents seized and searched Mr. Johnson's 13-year-old son's cell phone. They

did so even though the Search Warrant did not authorize the seizure and search of Mr. Johnson's children's cell phones. In addition, the Affidavit does not indicate that the government had any probable cause to believe that Mr. Johnson's son was at all involved in the events of January 6th, let alone was using his cell phone at the U.S. Capitol that day, and there is no indication that the eldest son consented to the seizure and search of his phone. *See id.* at 3. The contents of Mr. Johnson's cell phone, Person-1 , and his eldest son's cell phone are all backed up on a cloud computing service, and the account for all of the cell phones is in Mr. Johnson's name. As a result, a search of Person-1 cell phone or his son's cell phone is a search of Mr. Johnson's cell phone.

Cell Phones contain vast quantities of private, sensitive data, and information.

Cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 573 U.S. 373, 385 (2014). Indeed, 97% of Americans own a cell phone, and 85% of Americans specifically own a smartphone. Pew Rsch. Ctr., *Mobile Fact Sheet* (Apr. 7, 2021), https://www.pewinternet.org/fact-sheet/mobile/.

Cell phones and smartphones "differ in both a quantitative and a qualitative sense from other objects" because they "place vast quantities of personal information literally in the hands of individuals." *Riley v. California*, 573 U.S. 373, 386, 393. They are "minicomputers that also happen to have the capacity to be used as a telephone" and "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Id.* at 393. Not to mention many smartphone users download mobile applications (or "apps"), for which the names alone may reveal private information about the user. *See id.* at 397. All of the data a cell phone gathers may be stored locally on the phone or on a remote server (*e.g.*, in the cloud), with users oftentimes not knowing which. *Id*. The data on a phone "can date back to

the purchase of the phone, or even earlier" when users store their data to the cloud. *Id.* Because cell phones are used in a myriad of ways gather vast swaths of information and data and provide access to this information and data, they "reveal much more in combination than any isolated record," which have serious constitutional implications for "an individual's privacy interests or concerns." *Id.* at 394–95.

Potentially Privileged Communications and Documents on the Seized Electronic Devices

Since February 2017, Mr. Johnson has been involved in divorce, custody, child support proceedings, and Child Protective Services ("CPS") proceedings in Virginia state court. Mr. Johnson retained counsel to represent him in these family law proceedings. His son also had two different guardians *ad litem* appointed for him in the custody and CPS proceedings. Mr. Johnson used his mobile phones to communicate with his attorneys and his son's guardians *ad litem*, via e-mail and text messages. He also used his mobile phones to take photographs and gather documents at the instruction of his attorneys. In addition, Person-1, at Mr. Johnson's or his attorneys' instruction and, corresponded with Mr. Johnson's attorneys about the family law proceedings and sent them documents or other evidence implicated in the proceedings. All of these communications and documents are protected by attorney-client privilege, work product doctrine, or both.

On July 12, 2021, counsel for Mr. Johnson first alerted the government that there were potentially privileged communications and documents on the cell phones seized from Mr. Johnson. Counsel for Mr. Johnson took the position that a Special Master, not a Filter Team, should review the results of the search of the cell phones (and desktop computer) for any privilege materials; the government contended that review by a Filter Team is sufficient. After counsel for Mr. Johnson exchanged emails and engaged in telephone conversations about the potentially privilege materials

on the seized cell phones, the government agreed not to search the devices until it received an order from the Court with instructions on how to conduct the privilege review.[1]

ARGUMENT

A. The government illegally seized Mr. Johnson's desktop computer, walkie-talkies, and cameras in violation of the Fourth Amendment.

When a search warrant does not detail an item to be seized or details an item but does provide sufficient probable cause to search for the item, the government's seizure of that item is unconstitutional. *See, e.g.*, *Groh v. Ramirez*, 540 U.S. 551, 554 (2004) (holding that a warrant that did not describe the things to be seized unconstitutional); *United States v. Griffith*, 867 F.3d 1265, 1272 (D.C. Cir. 2017) (concluding that law enforcement did not have probable cause to search a home for "electronic devices apart from cell phones, including computers, tablets, and personal digital assistants" where the search warrant affidavit "provided no reason to suppose that [the subject of the warrant] possessed any of those devices or that any would be found in [his home]").

Here, both the Affidavit in support of the Search Warrant and Attachment A to the Affidavit sought to seize and search only the "[m]obile devices in the possession of P. JOHNSON and [redacted] Person-1 (or hereinafter 'the SUBJECT DEVICES')." Ex. 2, Maldonado Aff. ¶ 3(d); *Id.* Attach. A ("The devices to be searched are mobile phones in the possession of P. JOHNSON and [redacted] Person-1, or mobile devices located at the SUBJECT RESIDENCE available for use by P. JOHNSON or Person-1). The Affidavit then details the records and information the government has probable cause to believe it will find in the Subject Devices, *i.e.*, Mr. Johnson's and Person-1 mobile phones. *See id.* at ¶¶ 79–80. The Affidavit is, however, conspicuously

[1] Because the government agreed not to search the cell phones and other electronic devices until it received an order from the Court regarding how to conduct its review of protected documents, Mr. Johnson decided not to file a motion for a temporary restraining order and/or preliminary injunction in an effort to avoid needless, expensive, and time-sensitive litigation.

silent on the evidence the government had probable cause to believe it would find on the impermissibly seized desktop computer, HD cameras, and walkie-talkies. Indeed, the Affidavit details facts only related to Mr. Johnson's and Person-1 use of their cellular phones on January 6th, (*see id.* at ¶¶ 74–75) (describing Mr. Johnson's and Person-1 use of cell phones captured on open-source video)—the rest of the information pertaining to other types of electronic devices is mere speculation:

> Your Affiant is aware that individuals commonly take photographs and videos utilizing personal wireless telephones. Information 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. For example, I know based on my training and experience that such devices *may* contain evidence of internet searches, communications, and media indicative of motive, planning, coordination, intent, travel, and/or the purchase of clothing or other items of evidentiary value.

Id. at ¶ 76 (emphasis added).

The Affidavit provided no reason to believe that Mr. Johnson possessed any of these devices or that they would be found in his home, nor does it mention digital cameras or walkie-talkies. In short, the government provided no reason to believe that computers, mobile storage devices, or other electronic device would be found in Mr. Johnson's home, and it only sought and obtained approval to seize Mr. Johnson's and Person-1 cellphones. Thus, the government was not authorized to seize (and most certainly cannot search) the desktop computer, HD cameras, and walkie-talkies found at Mr. Johnson's residence. The government's proposed search is thus unconstitutionally overboard and the Court should find this part of the Search Warrant in violation of the Fourth Amendment.

B. Under the Fourth Amendment, the government must have probable cause to search the electronic devices and the data they contain.

The Fourth Amendment requires the government to have probable cause to search a cell phone. *See Riley*, 573 U.S. at 381. But separate probable cause is required to search each of the different types of data and other information stored on a cell phone. *See id.* at 394–5, 397. Put another way, probable cause to search or seize one type of data stored on a cell phone does not authorize the government to access all of the contents of a cell phone. Thus, to prevent unconstitutionally overboard and unreasonable searches, the government must specifically articulate the type or types of data for which it has probable cause to search.

Here, the government has failed to articulate with sufficient particularity the data and information to be searched and seized on the electronic devices, casting an unconstitutionally overbroad dragnet for information. Assuming *arguendo* that the Search Warrant is not unconstitutionally overbroad, the government can only search for documents and communications not protected by attorney-client privilege or work product doctrine.

1. The government's proposed search of the seized cell phones is not based on probable cause and is unconstitutionally overbroad.

The Founders enacted the Fourth Amendment to prevent general searches, that is, "a general, exploratory rummaging in a person's belongings." *Matter of the Search of Info. Associated with [redacted]@mac.comthat is Stored at Premises Controlled by Apple, Inc.*, 25 F. Supp. 3d 1, 6 (D.D.C. 2014) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). Search warrants must, therefore, raise a "fair probability" or a "substantial chance" that evidence of a crime will be found in the place to be searched for there to be probable cause. *Safford Unified Sch. Dist. No. 1 v. Redding*, 557 U.S. 364, 371 (2009). A constitutionally valid search warrant has four elements: (1) probable cause; (2) an oath or affirmation; (3) a particularized description of the place to be searched; and (4) a particularized description of the things to be seized. *Groh*, 540 U.S.

at 557 ("The Fourth Amendment states unambiguously that 'no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing* the place to be searched, and *the . . . things to be seized*.'") (emphasis in original). The particularity requirement is especially important now that cell phone storage of private, personal information in a single location "increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs." *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009); *see also Riley*, 573 U.S. at 396–97 ("[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.") (emphasis in original).

In this case, the April 12, 2021 Search Warrant is overbroad and lacks sufficient particularity with regard to the government's search of the seized Subject Devices in violation of the Fourth Amendment. Mr. Johnson does not contest the government's ability to seize the Subject Devices; rather, Mr. Johnson challenges the unlimited scope of the search of his devices. If there is probable cause to search the Subject Devices for evidence, the government can only look at the data and information on the mobile devices where it has probable cause to believe evidence may be found.

Not only do the Affidavit and its Attachments fail to specify the data and information to be searched, but they fail to provide a specific factual basis connecting each category of data and information on the Subject Devices to the crimes with which Mr. Johnson is charged.

The Affidavit arguably only identifies potential video from the events of January 6th on the cell phone Mr. Johnson was using that day and a text message he allegedly sent to an anonymous witness the following day. Ex. 2, Maldonado Aff. ¶¶ 73–74. It does not identify any apps, internet searches, photos, or other types of data and information potentially stored on the cell

phones seized from Mr. Johnson. Similarly, the Affidavit only notes Person-1 use of two cell phones on January 6th, one of which she purportedly used to listen to what the affiant believes were congressional proceedings. The affiant further attests that a different anonymous witness recalled Person-1 "posting photos and/or videos from the U.S. Capitol on [redacted] Facebook page." *Id.* at ¶ 73. Yet, the Affidavit:

> [S]ubmits that there is probable cause to believe that there exists physical and/or electronic evidence related to the commission of the offenses [with which Mr. Johnson is charged] on the mobile telephones and other electronic devices used by [Mr. Johnson and Person-1], including photographic, video, and other electronic evidence indicative of [Mr. Johnson's and Person-1] movements, location, motivation, planning, and communications related to the offenses listed herein, and the identities of co-conspirators and other individuals violating federal law during their entry into the U.S. Capitol, among other things.

Id. at ¶ 78.

It also broadly seeks "permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found within the SUBJECT DEVICES, in whatever form they are found." *Id.* at ¶ 79. The affiant then attests that there is probable cause to believe that the records and information described in Attachment B will be stored on the Subject Devices. *Id.*

Attachment B details a laundry list of evidence that the affiant purportedly has probable cause to believe the government with find on the Subject Devices without regard to whether there was probable cause to search each of these categories of information and data, including but not limited to: (1) "who used, owned, or controlled the SUBJECT DEVICES at the time the things described in the warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence"; (2) "evidence of the times the SUBJECT DEVICES [were] used"; and (3) "records of information

about the SUBJECT DEVICES' Internet activity, including firewall logs, caches, browser history and cookies, 'bookmarked' or favorite web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses." *Id.* Attach. B ¶ 4(a), (e), (i). Indeed, Attachment B only addresses the "items to be seized." *See id*. With regards to the search of the items seized, Attachment B states that it "authorizes review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant." *Id.* Attach. B at 58. It does not specify the type of data or information to be searched, nor the time frame for the search.

The government's Search Warrant is an unconstitutional general warrant. It proposes a wide-ranging search of the all the information and data contained on the seized electronic devices without regard to whether there is probable cause to search all of it. To have probable cause, the government must "know if specific information is contained on a device before searching it," and those searches are limited to the those aimed at uncovering evidence of a specific crime. Orin Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech. L. Rev. 1, 3 (2015). If the government is permitted to "search the entire electronic haystack for the needle" it "may see all the information the [entire] haystack reveals along the way," rendering the search of all data on a phone a general warrant. *Id.*; *see also Riley*, 573 U.S. 373, 396–97 (quoting *United States v. Kirschenblatt*, 16 F.2d 202, 203 (C.A.2) (noting that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him"); *Griffith*, 867 F.3d at 1275 ("[A] warrant with an 'indiscriminate sweep' is 'constitutionally intolerable.'" (quoting *Stanford v. Texas*, 379 U.S. 476, 486 (1965)).

But this is exactly what the government's proposed search of the seized electronic devices would do—rifle through the cell phones and desktop computer for any and all incriminating evidence against Mr. Johnson. This search would, in fact, go even further because cell phones contain "a broad array of private information never found in a home in any form." *Riley*, 573 U.S. at 396–97. Because the unconstitutionally broad Search Warrant in this case goes even further than the general warrants our Founding Fathers were concerned about, the appropriate remedy is the suppression of any and all electronic evidence the government seized. *See Taylor v. State*, 2021 WL 4095672, at *10 –11 (Del. Sept. 8, 2021) (holding that a warrant that authorized the search of "[a]ny and all store[d] data" of the digital devices, used "including but not limited to" language, and that "did not limit the search of [the] cell phone to any relevant time frame" failed to "describe the items to be searched for and seized with as much particularity as the circumstances reasonably allow and is no broader than the probable cause on which it is based").

"Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.' The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Riley*, 573 U.S. at 403 (citation omitted). Mr. Johnson respectfully requests that the Court uphold these constitutional protections and suppress any and all electronic evidence on the seized electronic devices, including evidence on the desktop computer, the imaged version of Person-1 cell phone, and his eldest son's cell phone (whether found through a manual search or by a search of the imaged phone).

2. Assuming *arguendo* that the Search Warrant is not unconstitutionally overbroad, the government can only search for materials not protected by attorney-client privilege or work product doctrine.

The attorney-client privilege is "the oldest of the privileges for confidential communications known to the common law." *In re Search Warrant Issued June 13, 2019*, 942

F.3d 159, 172–73 (4th Cir. 2019) (quoting *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981)), *as amended*, (Oct. 31, 2019). The client is the holder of the privilege, which allows him "to refuse to disclose and to prevent any other person from disclosing confidential communications between him and his attorney." *Id.* (quoting Black's Law Dictionary 129 (6th ed. 1990)). Similarly, work-product doctrine, protects "certain materials prepared by an attorney acting for his client in anticipation of litigation." *Id.* at 173–74 (internal quotation marks omitted) (quoting *United States v. Nobles*, 422 U.S. 225, 237–38 (1975)). This is a qualified privilege that is held by both the attorney and the client. *In re Search Warrant Issued June 13, 2019*, 942 F.3d at 174.

As detailed above, since February 2017, Mr. Johnson has been involved in divorce, custody, child support proceedings, and CPS proceedings in Virginia state court, and. Mr. Johnson retained counsel to represent him in these proceedings. In addition, his son also had two different guardians *ad litem* appointed for him in the custody and CPS proceedings. Mr. Johnson used his mobile phones to communicate with his attorneys and his son's guardians ad litem, via email and text messages. He also used his mobile phones to take photographs and gather documents at the instruction of his attorneys. Person-1, at Mr. Johnson's or his attorneys' instruction and, corresponded with Mr. Johnson's attorneys about the family law proceedings and sent them documents or other evidence implicated in the proceedings. All of these communications and documents are protected by attorney-client privilege, work product doctrine, or both. The government's review of any of any of these privileged materials would seriously injure Mr. Johnson, his counsel, or both. *Id.* at 175.

3. If the government can conduct a blanket search of the seized electronic devices, then a special master should be appointed to review the electronic evidence and separate out any potentially protected materials.

The government proposed—and the Search Warrant authorized—the use of a Filter Team to separate out any potentially privileged materials on the Subject Devices. The government's

position overlooks the fact that there is "an obvious flaw in the [filter] team procedure: *the government's fox is left in charge of the* [*defendant's*] *henhouse*, and may err by neglect or malice, as well as by honest differences of opinion. *In re Search Warrant Issued June 13, 2019*, 942 F.3d at 177–78 (first alteration in original) (quoting *In re Grand Jury Subpoenas*, 454 F.3d 511, 523 (6th Cir. 2006)), *as amended*, (Oct. 31, 2019). Here, the potentially privileged materials at issue date back to February 2017 and involve four separate attorneys, Person-1 [redacted], and his son. A filter team member, who has no first-hand knowledge of the underlying family law cases, can only guess as to the nature of the relationships and circumstances of the representation. No one in that position can appropriately protect privilege. The use of a filter team without this necessary firsthand knowledge also increases the risk of negligent disclosure of privileged materials or differences in opinion regarding whether materials are privileged or not. Given that, such a complicated privilege and work-product review is best left to a neutral special master—not Mr. Johnson's filter-team adversary. The fox ought not be left in charge of guarding the henhouse.

The Department of Justice's own policies regarding the search of potentially privileged materials seized from an attorney acknowledge that "a privilege team, a judicial officer, or a special master" may review the seized materials. Dep't of Justice, *Justice Manual* 9-13.420.F – Searches of Premises of Subject Attorneys, https://www.justice.gov/jm/jm-9-13000-obtaining-evidence#9-13.420 (updated Jan. 2021).[2] Although this policy governs materials seized from an attorney, the same privilege protections apply to seized materials whether in the attorney's possession or in the

[2] Relatedly, DOJ's own guidelines acknowledge that there are "three options" for the review of computer files for privileged material: (1) *in camera* review by the court; (2) review by a special master; and (3) review by a filer team. Computer Crime and Intellectual Property Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* at 110, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf. However, the guidelines acknowledge that "typical choice" is between a filter team and a special master. *Id.*

client's possession. Appointing a special master to review materials seized from the client is, therefore, a natural extension of DOJ's own policies and ensures that a neutral party—not an adversarial one—determines privilege.

The government must acknowledge that its own policies contemplate judicial review of privileged materials. The government cannot distinguish the Justice Manual's provisions governing searches of the premises of attorneys by arguing that it is the place searched (*i.e.*, a lawyer's office), instead of the items to be searched (*i.e.*, potentially privileged material), that matters. The holding of *In re Search Warrant* turns on the items searched—not the place searched. *See In re Search Warrant Issued June 13, 2019*, 942 F.3d at 177–78.

Moreover, the section of the *Justice Manual* cited above clearly governs the "review procedures" for the "materials seized," and not the place to be searched. It strains credulity to think that if potentially privileged materials were seized from a location other than an attorney's office that the government would not apply a similarly rigorous protocol to the review of those materials to avoid compromising its investigation.

Accordingly, if the Court authorizes a search of the seized electronic devices, then it should appoint a special master to review the electronic evidence and separate out any potentially protected materials.

CONCLUSION

WHEREFORE, for the reasons stated above, Mr. Johnson respectfully requests that the Court suppress all electronic evidence seized pursuant to the April 12, 2021 Search Warrant because it did not authorize the seizure of the desktop computer, HD cameras, and walkie-talkies, and it proposes an unconstitutionally overbroad and unreasonable search of the seized cell phones. Alternatively, Mr. Johnson requests that the Court appoint a neutral special master to review and

segregate documents and communications that are potentially protected by attorney-client privilege or the work product doctrine.

Dated: November 19, 2021

Respectfully submitted,

/s/

Kobie Flowers (Bar No. 991403)
BROWN GOLDSTEIN & LEVY, LLP
1717 K Street, NW, Suite 900
Washington, DC 20006
Tel: (202) 742-5969
Fax: (202) 742-5948
kflowers@browngold.com

Monica Basche (Bar No. MD0105)
BROWN GOLDSTEIN & LEVY, LLP
120 E. Baltimore Street, Suite 2500
Baltimore, Maryland 21202
Tel: (410) 962-1030
Fax: (410) 385-0869
mbasche@browngold.com

Counsel for Paul Russell Johnson

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a copy of this pleading was served on all counsel of record via the Court's electronic filing service.

Date: November 19, 2021

/s/ Kobie Flowers
Kobie Flowers