UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

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

INTRODUCTION

Paul Russell Johnson seeks to suppress certain electronic devices—and information and data contained on some of those devices—that were unlawfully seized from him on April 13, 2021 in the pre-dawn raid of his home in violation of the Fourth Amendment. 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.

ARGUMENT

I. The government did not have probable cause to seize the Explore One HD cameras, nor could it have relied in good faith on the Search Warrant to seize the walkie-talkies.

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 and the item must be suppressed from evidence.[1] *See, e.g.*, *Groh v. Ramirez*, 540

[1] If the government does not intend to introduce evidence from the Lenovo IdeaCentre Desktop Computer at trial, then Mr. Johnson concedes that his Motion to Suppress with regard to this evidence is moot. However, Mr. Johnson reserves the right to challenge any derivative use of

U.S. 551, 554 (2004) (holding that a warrant that did not describe the things to be seized was unconstitutional). However, the government may, under certain circumstances, evade the restrictions the Fourth Amendment places on its unwarranted intrusions into a person's private life through the good faith exception to the warrant requirement set forth in *United States v. Leon*, 468 U.S. 897 (1984). Under the good faith exception, the government may rely on the probable cause determination the magistrate judge made in approving the search warrant when conducting its search. *Id.* at 922. There are, however, four situations to which the good faith exception does not apply because the government had "no reasonable grounds to believe that the warrant was properly issued":

> (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).

A. The FBI agents did not have probable cause to seize the Explore One HD cameras.

As a threshold matter, the government did not even have probable cause to be at the location from which it seized the Explore One HD Cameras. The FBI agents searched for and seized items from Address-2 instead of Address-1,[2] the address listed on the Search Warrant.

---

evidence from the Lenovo IdeaCentre Desktop Computer as fruit of the poisonous tree. *See Nix v. Williams*, 467 U.S. 431, 441 (1984) (describing the "fruit of the poisonous tree" doctrine).

[2] Due to the highly publicized nature of the January 6th cases, these addresses are redacted for the privacy, safety, and security of Mr. Johnson and his family.

(*Compare* (Motion to Suppress Electronic Evidence or, in the Alternative, to Appoint a Special Master ["Mot. to Suppress"] Ex. 1, ECF No. 66-1, *with* (Ex. 1, GIS map of properties).

Contrary to the government's assertions, the Explore One HD cameras are not mobile devices. (Govt's Opp'n to Def.'s Mot. to Suppress Electronic Evidence or, in the Alternative, to Appoint a Special Master ["Govt's Opp'n"] at 10, ECF No. 63).[3] Attachment A to the Search Warrant Affidavit defines "Subject Devices," in relevant part, as "mobile devices located at the SUBJECT RESIDENCE available for use by P. JOHNSON or [Person-1]." (Motion to Suppress Electronic Evidence or, in the Alternative, to Appoint a Special Master ["Mot. to Suppress"] Ex. 2, Maldonado Aff., Attach. A at 53, ECF No. 66-2). Two of the defining characteristics of mobile devices are: (1) "[a]n operating system that is not a full-fledged desktop or laptop operating system"; and (2) "[a]pplications available through multiple methods (provided with the mobile device, accessed through a web browser, acquired and installed by third parties.)" M. Souppaya & K. Scarfone, NIST Special Publication 800-124 Revision 1, *Guidelines for Managing Security of Mobile Devices in the Enterprise* at 2 (June 2013), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf. The Explore One HD cameras do not have an operating system, nor do they have applications installed on them. *See* ExploreOne 1080P HD Action Camera with Wi-Fi Item 245002, Amazon.com, https://www.amazon.com/ExploreOne-1080P-Action-Camera-2450002/dp/B08GX89GRY (last visited Dec. 7, 2021). Moreover, a common sense understanding of the term "mobile devices"

[3] The government characterizes the Explore One HD Cameras as "mobile devices" based on a description of the cameras' capabilities on Amazon.com. (Govt's Opp'n to Def.'s Mot. to Suppress Electronic Evidence or, in the Alternative, to Appoint a Special Master ["Govt's Opp'n"] at 10 n.5, ECF No. 63). But this citation only addresses the "mobile" portion of the term; as explained by the National Institute of Science and Technology ("NIST") *infra*, the fact that the cameras are mobile does not necessarily make them mobile devices.

encompasses smartphones, tablet computers, and the like, not standalone digital cameras. The government's definition, by contrast, would encompass anything a person could reasonably carry. In short, the cameras are not the "mobile devices" contemplated in Attachment A to the Affidavit.

Next, the government contends that the Explore One HD cameras could be seized under Paragraph 3 of Attachment B to the Search Warrant Affidavit, which details the items to be seized. This argument similarly has no merit. The first Paragraph 3[4] states: "Records and information—including but not limited to documents, communications, emails, online postings, photographs, videos, calendars, itineraries, receipts, and financial statements . . ." (Maldonado Aff., Attach. B at 55). Assuming that the cameras are mobile devices (they are not), this paragraph does not authorize their seizure simply because it includes records and documents that may be available in digital format. The government must have probable cause to seize a device that contains such information and records in the first instance, and the Affidavit fails establish it. It is bereft of any references to Mr. Johnson using a camera on January 6th (in comparison to the references to Mr. Johnson using a cell phone). Yet, the government points to Paragraph 76 of the Affidavit, which states:"[i]nformation from wireless phones may also be saved or backed up on computers, mobile storage devices, or other electronic devices," (Govt's Opp'n at 11 (citing Maldonado Aff. ¶ 76)), to argue that it was authorized to seize the cameras. But common sense dictates that mobile phone users are not backing up or saving their pictures and videos to a separate digital camera—they are either saving them to a personal computer or to the cloud. In addition, the Affidavit contains no specific factual averments that someone witnessed Mr. Johnson backing up photos or video to a digital camera. *Cf. United States v. Smith*, No. CR 19-324 (BAH), 2021 WL 2982144, at *7

[4] Attachment B to the Affidavit contains two Paragraph 3s. (*See* Maldonado Aff., Attach. B at 55–56).

(D.D.C. July 15, 2021) ("The affidavit provided ample grounds to believe that defendant committed [the charged offense] and that incriminating evidence regarding that suspected offense would be found on his cell phone and his computer to which he connected his cell phone and A.S.'s cell phone."). Thus, it is unreasonable to conclude that Mr. Johnson backed up or saved photos or videos to a digital camera.

The Affidavit also does not establish probable cause to believe that Mr. Johnson possessed a camera on January 6, 2021. The government relies on statements from a YouTube video in which Mr. Johnson purportedly stated, "I have video where I'm slinging him around." (Govt's Opp'n at 12 (citing Maldonado Aff. ¶¶ 54, 74)). But, given the averments in the Affidavit related to Mr. Johnson's and Person-1's cell phone usage on January 6, 2021, it is not reasonable to conclude that such video footage could be found on a digital camera, especially given the ubiquity of cell phones.[5]

B. The FBI agents could not have relied in good faith on Attachment B to the Search Warrant to seize the walkie-talkies.

The *Leon* good faith exception to the warrant requirement does not apply to the seized walkie-talkies. "Courts have allowed more latitude in connection with searches for contraband items like 'weapons [or] narcotics.' But the understanding is different when police seize 'innocuous" objects,' *United States v. Griffith*, 867 F.3d 1265, 1276 (D.C. Cir. 2017) (quoting *Stanford v. Texas*, 379 U.S. 476, 486 (1965)), like the walkie-talkies at issue here. A search that encompasses innocuous objects calls for "special care" such that it "minimizes unwarranted intrusions upon privacy.'" *Id.* (quoting *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976)).

[5] Mr. Johnson does not contest that "people who spend time at a particular address also store their belongings and devices as part of their daily lives at the address." (Govt's Opp'n at 12 (citing Maldonado Aff. ¶ 71)). Rather, Mr. Johnson challenges the seizure of the Explore One HD cameras as outside the scope of the Search Warrant.

And the warrant "must be tailored to the justifications for entering the home." *Id.* Here, the Search Warrant was not so narrowly tailored, particularly with regard to the walkie-talkies. This places the Search Warrant squarely under the third situation to which the *Leon* good faith exception does not apply—it "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable" *Leon*, 486 U.S. 897 at 923. In analyzing this type of situation, courts consider "whether an objectively reasonable officer could think the affidavit established probable cause." *Griffith*, 867 F.3d at 1278. In this case, it was objectively unreasonable to think that the Affidavit established probable cause to seize the walkie-talkies.

First, the Affidavit is silent on walkie-talkies and their use by Mr. Johnson on January 6th, and instead poses a hypothetical scenario under which they "could have been used by co-conspirators to communicate during the unlawful entry into the U.S. Capitol." (Maldonado Aff., Attach. B ¶ 1(k), Ex. 2). But the Affidavit lacks any allegations that Mr. Johnson used a walkie-talkie on January 6th, and he never entered the U.S. Capitol. Put simply, there is no probable cause to believe that Mr. Johnson used walkie-talkies in connection with the charges against him. *See Griffith*, 867 F.3d at 1278 (rejecting the government's good faith exception argument and granting the defendant's motion to suppress where the affidavit "provided no explanation at all of whether [the defendant] might own a phone or whether any such phone might be in his home").

Second, the FBI searched Address-2 instead of Address-1, the address listed on the Search Warrant. (Ex. 1, GIS map of properties). It is presumptively unreasonable under the Fourth Amendment to search a house for which no search warrant was issued. *Corrigan v. D.C.*, 841 F.3d 1022, 1029 (D.C. Cir. 2016) (quoting *Payton v. New York*, 445 U.S. 573, 586 (1980)). In addition, the walkie-talkies were inside of a locked safe, (Ex. 2, Johnson Aff. ¶¶ 13), and nothing in the Search Warrant or Affidavit authorized the FBI agents to open the safe.

II. Mr. Johnson has established standing to contest the seizure and search of Person-1's cell phone.[6]

Mr. Johnson has a subjective and legitimate expectation of privacy in the contents of Person-1's cell phone. Two factors point to this expectation: Mr. Johnson's possessory interest in the phone, and the quality of the private information contained in the phone.

Mr. Johnson bought Person-1's phone and pays the monthly bills for it, including the month of April 2021 when the FBI searched the phone. When Mr. Johnson is unable to use his primary cell phone, he uses Person-1's cell phone to manage his personal and business affairs. (Ex. 2, Johnson Aff. ¶ 10). The government cites the unreported case *United States v. Dore*, 586 F. App'x 42, 46 (2d Cir. 2014), to argue that Mr. Johnson has no ownership or possessory interest in Person-1's cell phone. (Govt's Opp'n at 15). But unlike in that case, here Mr. Johnson has submitted an affidavit attesting to the above facts and affirming their truthfulness. (*See* Ex. 2, Johnson Aff.). He has "offer[ed] testimony to establish that he had an ownership or cognizable property interest in the cellphone at issue." *United States v. Hamlett*, No. 3:18-cr-24 (VAB), 2018 WL 4656241, at *5 (D. Conn. Sept. 27, 2018).

In addition to Mr. Johnson's possessory interest in Person-1's cell phone, the quality of the information contained on the cell phone buttresses his assertion that he has "a privacy interest in the cell phone[] in some other manner." *Dore*, 586 F. App'x at 46. Person-1's phone is essentially a mirror of Mr. Johnson's primary phone. (Ex. 2, Johnson Aff. ¶¶ 7, 8). It is permanently logged in to his personal and business email accounts. (Ex. 2, Johnson Aff. ¶ 8). It has saved on it the usernames and passwords for Mr. Johnsons personal savings account, his business checking

[6] If the government did not seize evidence from his son's cell phone and does not intend to introduce evidence from the device at trial, then Mr. Johnson concedes that his Motion to Suppress with regard to his son's cell phone is moot. However, Mr. Johnson reserves the right to challenge any derivative use of evidence from his son's cell phone as fruit of the poisonous tree. *See Nix*, 467 U.S. at 441 (describing the "fruit of the poisonous tree" doctrine).

account, and his two business loan accounts. (Ex. 2, Johnson Aff. ¶ 6). The only way Mr. Johnson can access his business loan accounts is through the saved usernames and passwords on Person-1's phone. (Ex. 2, Johnson Aff. ¶ 6(e)). The same is true of Mr. Johnson's child support account. (Ex. 2, Johnson Aff. ¶ 6(f)). Person-1's phone even has software called "If This Then Then That" installed, which allows Person-1's phone to see any message, email, or voice mail that goes to Mr. Johnson's phone. (Ex. 2, Johnson Aff. ¶7). Person-1's phone also contains privileged communications with Mr. Johnson's attorneys and information that is work product. (Ex. 2, Johnson Aff. ¶ 6(b)). Essentially, Person-1's phone contains the information Mr. Johnson needs to lead his life. In some cases, it is the only place where that essential information can be found.

"The fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018). The Court in *Carpenter* held that the defendant maintained a legitimate expectation of privacy in the record of his physical movements as captured through cell-site location information ("CSLI"). *See* 138 S. Ct. at 2219 (noting that the government "invaded [the defendant's] reasonable expectation of privacy in the whole of his physical movements."). While CSLI merely reveals one's location, the information on Person-1's phone reveals the most intimate aspects of Mr. Johnson's life including his medical affairs, his legal affairs, his e-mail messages, and his text messages. He only "shared" it with a third party to the extent that the information resided on another cell phone in which he also had a possessory interest. Just as the Supreme Court held in *Carpenter* that a person has a has a right to privacy in the records maintained by MetroPCS and Sprint, Mr. Johnson has a right to privacy in the information contained on Person-1's cell phone.

III. The Search Warrant is overbroad and insufficiently particular with regard to the electronic data to be seized from Mr. Johnson's cell phones in violation of the Fourth Amendment.

The government contends that the Search Warrant sufficiently limits the permissible search of the seized cell phones and identifies with particularity the information to be seized pursuant to that search.[7] (Govt's Opp'n at 19–20). The government overlooks the fact that the Affidavit and its Attachments do not place any meaningful limitations on the types of data and information to be seized from the cell phones. 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). Separate probable cause is required to search each of the different types of data and other information stored on a cell phone. *See Riley v. California*, 573 U.S. 373, 394–5, 397 (2014).

Here, Attachment B states that the items to be seized are "fruits, evidence, information, contraband, or instrumentalities, *in whatever form and however stored*, of the charges alleged in the Indictment, "including, but not limited to" a laundry list of evidence. (Maldonado Aff., Attach.

[7] The government misunderstands Mr. Johnson's argument in two respects. First, the government characterizes Mr. Johnson's argument as a challenge to the manner in which the Search Warrant was executed, as opposed to a challenge to the insufficient particularity with which the Search Warrant describes the data and information to be seized from his cell phones.(Govt's Opp'n at 19). Mr. Johnson does not contend that the Search Warrant should detail a particular search protocol. Rather, he contends that the government must have separate probable cause to search each of the different types of data and information stored on or accessible through a cell phone. (Mot. to Suppress at 10). Second, the government contends that the Fourth Amendment does not prohibit it 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. (*Id.* at 20). But Mr. Johnson is not contesting the FBI agents' ability to seize the cell phones in his possession; he is contesting the fact that the government intends to search the seized phones for all types of data and information as overbroad and insufficiently particular.

B ¶ 1 at 54). Then, Paragraph 4 of Attachment B, which specifically addresses the Subject Devices, permits, without limitation:

> 4. For the **SUBJECT DEVICES**:
>
> a. evidence of who used, owned, or controlled the **SUBJECT DEVICES** at the time the things described in this 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;
>
> b. evidence of software, or the lack thereof, that would allow others to control the **SUBJECT DEVICES**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
>
> c. evidence of the attachment to the **SUBJECT DEVICES** of other storage devices or similar containers for electronic evidence;
>
> d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the **SUBJECT DEVICES**;
>
> e. evidence of the times the **SUBJECT DEVICES** was used;
>
> f. passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT DEVICES**;
>
> g. documentation and manuals that may be necessary to access the **SUBJECT DEVICES** or to conduct a forensic examination of the **SUBJECT DEVICES**;
>
> h. records of or information about Internet Protocol addresses used by the **SUBJECT DEVICES**;
>
> i. records of or 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.

The Affidavit does not establish that there is a reasonable probability that the government will find evidence, fruits, information, contraband, or instrumentalities of the offenses that Mr. Johnson is charged with in each of the above categories of information and data. For example, the Affidavit authorized the government to seize Mr. Johnson's emails, yet it contains no statements related to Mr. Johnson's use of email to commit the alleged offenses. In addition, the limitations placed on the categories of evidence in Paragraph 1 of Attachment B to the Affidavit are absent from

Paragraph 4, thus authorizing a wide-ranging search of all these types of data and information. This reading is supported by the fact that Subparagraph 4(a) mentions "the things described in this warrant," while none of the other Subparagraphs mentions the warrant. Further bolstering this reading is that Paragraph 4 authorizes the seizure of information not confined to the dates surrounding the charge offenses, like passwords, encryption keys, and user manuals.

Further, in making its argument, the government largely relies on older cases that pre-date *Riley* and *Carpenter*[8] and do not reflect the evolving law of digital device litigation. Many of the cases involve computers and computer-related crimes,[9] not cell phones, and therefore also do not accurately reflect the privacy concerns numerous courts have articulated with regard to cell phone searches. More recently, courts have started to recognize that the unique nature of cell phones requires that search warrants for electronic devices must articulate probable cause with regard to each category and type of data the government intends to seize. *See Taylor v. Delaware*, 260 A.3d 602, 615–6 (Del. 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" was overbroad and unconstitutional); *see also Riley*, 573 U.S. at 394–5, 397.

---

[8] In *Carpenter*, the U.S. Supreme Court reached important holdings with regard to the data gathered from cell phones. First, the Court held that an individual retains a legitimate expectation of privacy in cell-site records that capture his physical movements and, as a result, when the government obtains those records, it constitutes a search for the purposes of the Fourth Amendment. 138 S. Ct. at 2217. As such, the government must obtain a warrant supported by probable cause to acquire cell-site records. *Id.* at 2221.

[9] *See United States v. Ulbricht*, 858 F.3d 71 (2d Cir. 2017) (involving the search of a computer for evidence of computer crimes—the defendant was a hacker and was implicated in illegal transactions on the Silk Road); *United States v. Richards*, 659 F.3d 527, 538 (6th Cir. 2011) (child pornography case involving the search of a computer); *United States v. Burgess*, 576 F.3d 1078 (10th Cir. 2009) (same).

IV. The filter procedures detailed in the Search Warrant would not adequately protect the information and communications on Mr. Johnson's cell phones that are protected by privilege and/or work product.

The government contends that the use of a filter team is "a proper, fair, and acceptable method of protecting privileged materials in this case." (Govt's Opp'n at 23). But the government overlooks the case law to the contrary, particularly with regard to criminal proceedings. *See, e.g.*, *United States v. Gallego*, No. CR1801537001TUCRMBPV, 2018 WL 4257967, at *2 (D. Ariz. Sept. 6, 2018) ("[F]ederal courts have generally 'taken a skeptical view of the Government's use of [filter teams] as an appropriate method for determining whether seized or subpoenaed records are protected by the attorney-client privilege.'" (quoting *United States v. SDI Future Health, Inc.*, 464 F. Supp. 2d, 1027, 1037 (D. Nev. 2006))); *United States v. Kaplan*, No. 02 Cr. 883 (DAB), 2003 WL 22880914, at *4 n.4, * 12 (S.D.N.Y. Dec. 5, 2003); *United States v. Stewart*, No. 02 Cr. 395 (JGK), 2002 WL 1300059, at *6 (S.D.N.Y. June 11, 2002); *In re Search Warrant for L. Offs. Executed on Mar. 19, 1992*, 153 F.R.D. 55, 59 (S.D.N.Y. 1994) ("[R]eliance on the implementation of a [filter team], especially in the context of a criminal prosecution, is highly questionable, and should be discouraged."). In addition, contrary to the government's assertions, only the court in *United States v. Jackson*, No. CR.A.07-0035 (RWR), 2007 WL 3230140, (D.D.C. Oct. 30, 2007), applied the factors enumerated in the government's Opposition, and, as an unpublished opinion, *Jackson* is not binding on this Court.

Assuming *arguendo* that this Court will apply the four *Jackson* factors, they still weigh in favor of appointing a Special Master in this case. As to the first factor—whether the potentially privileged documents are already within the government's possession—although the government has seized Mr. Johnson's cell phones, it has not started its search of the data and information on those phones, and they (or their contents) could easily be turned over to the Special Master, as was the case in *In re Search Warrant.* The second factor—whether the lawfulness of the acquisition of

the documents to be reviewed was not initially challenged—weighs in Mr. Johnson's favor. Indeed, Mr. Johnson's counsel alerted the government as soon as he learned that there were potentially privileged and protected communications and information on Mr. Johnson's cell phones and requested the appointment of a Special Master at that time. Mr. Johnson is not an attorney and could not have known to challenge the seizure of his cell phones right after their seizure based on the fact that they contain potentially privileged materials. The third factor—whether there is a more extensive number of documents at issue—also weighs in Mr. Johnson's favor. As the information and communications the government seeks to search are in digital form, a search protocol can be developed to readily filter out potentially privileged and protected materials for review by the Special Master. As to the fourth factor—the use of a filter team's effect on the appearance of fairness—given the DOJ's unprecedented prosecution of 719 cases arising out of the events of January 6th, which marshals the resources of United States Attorneys' offices across the country and the politically charged nature of these prosecutions, appointing a Special Master would be appropriate to give the appearance of fairness. *See Gallego*, 2018 WL 4257967, at *2 ("[T]he use of walled-off taint teams undermines the appearance of fairness and justice.").

Next, contrary to the government's assertions, *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159, 172–73 (4th Cir. 2019), *as amended*, (Oct. 31, 2019), is directly relevant to this case. First, the inquiry is not whether the government is interested in Mr. Johnson's privileged or work-product protected communications—the government was not interested in the vast majority of the defendant's privileged communications in *In re Search Warrant*. 942 F.3d at 172 (noting that 99.8 percent of the 52,000 potentially privileged emails seized by the government were not relevant to the government's criminal case against the defendant). Perhaps more compelling here is that none of the potentially privileged materials are conceivably relevant to the government's

case against Mr. Johnson, thus counseling for even greater protection of these materials—and these materials should be given the full benefit of the protections that cover them. Second, as discussed above, the sweep of the Search Warrant with regard to the Subject Devices is so broad, that it cannot help but capture potentially privileged and protected materials. Finally, although the filter team protocols in this case differ from those in *In re Search Warrant*, they nevertheless fail to provide adequate protections for Mr. Johnson's (and his attorneys') privileged and protected materials. (Ex. 2, Johnson Aff. ¶ 6(b)). Here, under the Search Warrant's filter protocols, the Filter Team would review Mr. Johnson's materials and "provide all communications that are not potentially protected materials to the Prosecution Team." (Maldonado Aff., Attach. B 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, and the filter team may "have a more restrictive view of privilege" than Mr. Johnson and his counsel. *Gallego*, 2018 WL 4257967, at *2 The procedure in the Search Warrant permits the Filter Team—not the privilege holder—to determine what is privileged and what is not in the first instance. But this determination should be made by the privilege holder or a neutral party, like a special master, and not parties that may have a narrower view of privilege. As a result, the procedure detailed in the Search Warrant does not adequately protect privileged materials and leaves the government's fox in charge of Mr. Johnson's henhouse. *See In re Search Warrant Issued June 13, 2019*, 942 F.3d at 177–78.

The government also misunderstands Mr. Johnson's argument with regard to the *Justice Manual*. Mr. Johnson does not contend that he is entitled to the appointment of a Special Master based on the *Justice Manual's* provisions. Rather, Mr. Johnson contends that even the U.S. Department of Justice's own internal policies acknowledge the use of a filter team as one of the options for the review of potentially privileged materials, but it is not necessarily the default or the preferred option. Further, as Mr. Johnson noted in his Motion to Suppress, the appointment of a special master to review potentially privileged materials does not turn on the place searched—a subject attorney's premises—but on the items to be searched. *See In re Search Warrant Issued June 13, 2019*, 942 F.3d at 177–78. Similarly, with regard to the DOJ's guidelines for reviewing computer files, Mr. Johnson does not contend that they mandate the appointment of a special master; he simply notes that the DOJ's own policies acknowledge that the appointment of a special master as an option, and that the use of a filter team is not the default or preferred option.

Finally, the government argues that the Court should not give weight to Mr. Johnson's concerns over the filter team's lack of first-hand knowledge about his family law cases when Mr. Johnson has not given the government this information. (Govt's Opp'n at 27). This argument is a red herring. Mr. Johnson is not obligated to give the government information to assist in its privilege review, especially when the government knows that he will be contesting the manner in which the government proposes to conduct its review.

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: December 10, 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 I caused a copy of this pleading was served on all counsel of record via the Court's electronic filing service.

/s/ Kobie Flowers
Kobie Flowers

Date: December 10, 2021