Appeal No. 22-CF-0447

DISTRICT OF COLUMBIA COURT OF APPEALS

ROBERT WILSON DEAN, JR.,

Appellant,

v.

UNITED STATES OF AMERICA,

Appellee.

Appeal from the Superior Court of the District of Columbia
Criminal Division

BRIEF OF AMICUS CURIAE PUBLIC DEFENDER SERVICE IN SUPPORT OF APPELLANT

SAMIA FAM

FLEMING TERRELL

PUBLIC DEFENDER SERVICE
633 Indiana Avenue, NW
Washington, DC 20004

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

Statutes & Rules

Other Authorities

.

INTEREST OF AMICUS

This appeal presents constitutional questions of importance to criminal justice in the District of Columbia, and hence to the Public Defender Service and its clients. First, the Court must address the requirements of probable cause and particularity for cell phone search warrants consistent with *Burns v. United States*, 235 A.3d 758 (D.C. 2020). Second, it must decide, as an issue of first impression, whether authorities may lawfully render in readable format and expose to law enforcement's view the contents of all data on a cell phone when executing a warrant that authorizes them to search only for one month's worth of digital records.

SUMMARY OF FACTS & ARGUMENT

MPD Detective Richard Rice sought a warrant to conduct a full physical extraction and search of Mr. Dean's cell phone for "[a]ll records" and "[a]ny and all evidence related to the murder" that Mr. Dean was suspected of committing. *See* Appellant's Appx. D, Search Warrant ("2020 Warrant"), Attach. B(1)-(1)(a) (Jan. 30, 2020). Detective Rice's supporting affidavit detailed the factual basis to suspect Mr. Dean, including that he had exchanged several inculpatory texts and cell phone calls with a witness ("Witness 2") immediately before, and within two days after, the decedent was killed. *See* 2020 Warrant ¶¶ 10-16. Before signing the warrant, the judge wrote in a date range, limiting the authorization to search for "[a]ll records . . . that relate to the offense" to "3/1/2018 – 4/5/2018," the month preceding the offense up through Mr. Dean's arrest. 2020 Warrant, Attach. B(1).[1]

[1] The judge also crossed out three provisions apparently copied from an earlier warrant authorizing a search for evidence of a separate shooting in which Mr. Dean

This date range, however, is ten times longer than the three days for which the affidavit established probable cause to believe Mr. Dean exchanged texts and calls. *See infra* Part II.A. It did nothing, moreover, to limit the search to those categories of data, much less the specific communications with Witness 2 for which probable cause existed. This warrant was thus analytically indistinguishable from the warrant to search for "all records that relate to" a homicide that was invalidated as obviously overbroad and lacking in particularity in *Burns*, 235 A.3d at 769, 777-80.

Even if there could be any doubt that this warrant, too, was in effect a general warrant to rummage at will through the vast trove of private data on Mr. Dean's cell phone, it cannot survive even a cursory glance at the provision Detective Rice inserted at Paragraph 35 of the incorporated affidavit proclaiming authorities' "inten[t]" to "perus[e] *all* stored information" on the phone as they deemed "necessary" to find responsive evidence. 2020 Warrant ¶ 35 (emphasis added). The government claimed the warrant judge's signature "authorized" law enforcement to do just what Paragraph 35 says: "not only extract[] 'all stored information,' but also briefly review[] this stored information to respond to the warrant" (R.88 at 5). That is the very definition of a general warrant, and as such would make it undeniably clear to any reasonably well-trained police officer that this warrant was unlawful. The fruits of the resulting search must accordingly be suppressed. *Burns*, 235 A.3d at 778-79.

The manner in which law enforcement agents executed this warrant—and

---

was the victim. 2020 Warrant, Attach. B(1), (1)(b), (1)(d). Authorities "were no longer investigating" that shooting in 2020 (10/5/21 at 34).

according to the AUSA prosecuting this case, the manner in which they execute *every cell phone search warrant* (10/5/21 at 25, 27)—also raises constitutional concerns so grave as to require suppression. A Department of Forensic Services (DFS) analyst testified she used Cellebrite's "UFED" software application to "extract" a copy of all data from the phone, then used "another separate application called Cellebrite Physical Analyzer" to "take[] that extraction and decode[] it so that it sends the data in a human readable format" to be viewed "on the application," and finally, she "generate[d] a PDF report" containing all of the decoded data, including all "call logs, text messages, logs, Web browsing data, locations, pictures, video files, documents, [and] chat messages" from the phone (10/26/21 at 200-202).[2] Notwithstanding Attachment B's one-month date restriction on what records authorities could search for, and despite the Cellebrite software's capacity to filter which decoded data to include in the PDF report by date, as well as by type and even keyword,[3] either Detective Rice or the prosecutor picked up the full, unredacted,

---

[2] A version of the report redacted by the prosecutor (10/5/21 at 19-20) was introduced into evidence as Government Exhibit 501 (10/26/21 at 201-203). Undersigned counsel will file a motion to supplement the record on appeal with a copy of that exhibit.

[3] *See* Cellebrite, "Release Notes: UFED Physical Analyzer, UFED Logical Analyzer and Cellebrite Reader v7.20" at 3 (June 2019), *available at* https://cellebrite.com/wp-content/uploads/2019/06/ReleaseNotes_UFED_PA_7.20.pdf (last accessed June 16, 2023) (describing "one-click" function to "incorporate or exclude all items from a report . . . including adding events that occurred within a specific date range"); Cellebrite, "Release Notes: UFED Physical Analyzer, UFED Logical Analyzer and Cellebrite Reader v7.23" at 3 (Sept. 2019), *available at* https://cellebrite.com/wp-content/uploads/2019/09/ReleaseNotes_UFED_PA7.23_web.pdf (last accessed June 16, 2023) (describing capacity to conduct advanced

14,000-page extraction report from DFS, and the AUSA reviewed it for evidence with which to prosecute Mr. Dean (10/5/21 at 21-23). While she had no "specific" or "particular memory" of how she conducted that review, the AUSA proffered that in general "how I do all of my extractions and have been kind of instructed to [do them]" (10/5/21 at 21, 37) is to use the PDF's table of contents "to skip to the sections where [authorities] are allowed to go based on the [warrant's] Attachment B section," R.92 (Order Vacating Suppression Ruling) at 12 (citing 10/5/21 at 21-22, 25, 35-37). "I will continue to take that approach," she added, "not only in this case but in other cases as well" (10/5/21 at 37).

Regardless of which sections of the PDF the AUSA actually looked at, her receipt of a document translating every byte of data on the phone into readable text constituted a search that "provided an opportunity to 'rummage' through [Mr. Dean's] private information" at will, R.92 at 16-17, in clear violation of the Fourth Amendment. If not roundly condemned in this case, this approach to executing cell phone search warrants will neutralize any judge's attempt to restrict their search authorizations, eviscerating *Burns* and the bedrock Fourth Amendment principles of probable cause and particularity for which it stands.

Although the court below initially suppressed all fruits of the warrant to sanction the prosecutor's search beyond the date-limited scope of Attachment B (10/12/21 at 16-17), it reversed itself after the government argued the search was

---

keyword searches and "mark items" within results "to include in your report"). These capacities were included in software updates that issued before the extraction report in this case was generated, according to Government's Exhibit 501, using Cellebrite Physical Analyzer v7.29.0.152.

authorized by Superior Court Rule of Criminal Procedure 41(e)(2) and Paragraph 35's boilerplate language about the authorities' intended search methodology. *See* R.88 (Gov. Mtn. for Reconsideration), R.92 (Order Vacating Suppression Ruling).

Rule 41(e)(2), however, merely authorizes the seizure of computers and other digital storage devices, or a copy of their contents, to allow for an off-site digital search. *See* Sup. Ct. R. Crim. Proc. 41, cmt. to 2017 amendments. It explicitly requires that search be done "consistent with the warrant," Sup. Ct. R. Crim. Proc. 41(e)(2), and does not permit the search "process of identifying and segregating seizable electronic data" from the device or the digital copy of its contents "to bring constitutionally protected data into plain view." *United States v. Schesso*, 730 F.3d 1040, 1047 (9th Cir. 2013) (quotation marks, citation and alteration omitted).

To the extent Paragraph 35 can be read as granting law enforcement unfettered discretion to decode and gratuitously expose for the prosecutor's "perus[al]" all data on the phone despite Attachment B's date and content restrictions—and both the government's position below and its manner of executing this search indicate it did read Paragraph 35 that way—it is ineffectual. "The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant," *United States v. Ramirez*, 523 U.S. 65, 71 (1998), and it is manifestly unreasonable to expose the entire contents of a cell phone to police or the prosecutor when they have a warrant to search only for records from a one-month period. Because the manner in which authorities executed this warrant "flagrantly exceed[ed]" its already overbroad scope, suppression is doubly required. *United States v. Lewis*, 147 A.3d 236, 245 (D.C. 2016).

ARGUMENT

I. CELL PHONE SEARCH WARRANTS MUST FULLY COMPLY WITH THE FOURTH AMENDMENT'S WARRANTS CLAUSE.

This Court recognized in *Burns* that "[t]he privacy interests underlying the[] fundamental Fourth Amendment principles" of probable cause and particularity "may be at their most compelling when police wish to search the contents of a modern smart phone," a device that the Supreme Court has recognized contains "so much varied and sensitive information" that its search "'would typically expose to the government far *more* than the most exhaustive search of a house[.]'" 235 A.3d at 772-73 (quoting *Riley v. California*, 573 U.S. 373, 396 (2014)) (emphasis in *Riley*). The Warrants Clause's rules of probable cause and particularity—intended "to deny police the ability 'to rummage at will' through a person's private matters"—must therefore be applied as rigorously to the digital space of a cell phone's memory as the physical space of a house. *Id*. at 771 (quoting *Arizona v. Gant*, 556 U.S. 332, 345 (2009)). "Vigilance in enforcing the probable cause and particularity requirements is thus essential to the protection of the vital privacy interests inherent in virtually every modern cell phone and to the achievement of the 'meaningful constraints' contemplated in *Riley*." *Id*. at 773 (quoting *Riley*, 573 U.S. at 399).

Burns detailed what probable cause and particularity mean for a cell phone search warrant. For probable cause, it is "essential" that the warrant application "set forth" "particularized facts and circumstances" that provide "'a substantial basis'" to believe "not only that an item of [digital] evidence is likely to be found [on the phone], but also that there is a nexus between the item to be seized and the criminal behavior under investigation." *Id.* at 771-72 (quotation marks omitted) (citing

Illinois v. Gates, 462 U.S. 213, 239 (1983); *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967); *United States v. Griffith*, 867 F.3d 1265, 1271 (D.C. Cir. 2017); *United States v. McPhearson*, 469 F.3d 518, 524 (6th Cir. 2006)). Because the required nexus is between the offense and *data on the phone*, not the offense and the user, "[i]t is not enough" for a cell phone search warrant "to show there is probable cause to arrest the owner or user of [a] cell phone[.]" *Burns*, 235 A.3d at 773.[4] Neither will "bare bones" claims of probable cause "based on an affiant's 'training and experience'" or "suspicions, beliefs, or conclusions" do, as reliance on these would impermissibly reduce the warrant judge's role to that of "a rubber stamp for the police." *Burns*, 235 A.3d at 771-72 (quotation marks omitted) (citing *Gates*, 462 U.S. at 239; *Aguilar v. Texas*, 378 U.S. 108, 111 (1964); *United States v. Underwood*, 725 F.3d 1076, 1081 (9th Cir. 2013), *United States v. West*, 520 F.3d 604, 610 (6th Cir. 2008)). Instead, the affidavit in support of a cell phone warrant "must contain adequate supporting facts about the underlying circumstances to show that probable cause exists" to believe the phone's memory contains at least some

[4] *See also*, *e.g.*, *United States v. Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978) ("The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought."); *Griffith*, 867 F.3d at 1271 ("[P]robable cause to arrest a person will not itself justify a warrant to search his property."); *McPhearson*, 469 F.3d at 524 (search warrant application "must contain particularized facts demonstrating" a "nexus between the place to be searched and the evidence sought"); 2 Wayne R. LaFave, *Search & Seizure* § 4.6(a) (6th ed. 2022) ("[M]uch more" than probable cause to arrest is required for a search warrant; it must also "be probable (i) that the described items are connected with criminal activity, and (ii) that they are to be found in the place to be searched.");.").

data that is evidence of the crime under investigation. *Burns*, 235 A.3d at 772-73 (quotation marks and citation omitted). Applying these standards, the *Burns* court held that the warrant applications at issue there set out probable cause to search Burns's cell phones for "text messages between Mr. Burns" and the decedent on the night of the murder, "a log showing the precise time of the telephone call Mr. Burns reportedly made to his cousin (W-3) that night," and information from the phone's "GPS tracking features" about "Mr. Burns's whereabouts at pertinent times" that night and the following day. Beyond those "discrete items, the affidavits stated no facts that even arguably provided a reason to believe that any other information or data on the phones had any nexus to the investigation." *Id*. at 774.

"[P]robable cause to believe the phone contains *some* evidence of a crime," however, is "not enough," *id*. at 773 (emphasis added), to authorize an unbounded search for "any evidence" of that crime, *id*. at 774-75. This is where the particularity requirement plays a critical role in safeguarding the encyclopedic range of private information contained in the typical cell phone: The "warrant must specify the particular items of evidence to be searched for and seized from the phone and be strictly limited to the time period and information or other data for which probable cause has been properly established." *Id*. at 773. Merely "limiting the search to evidence of a particular crime" like the *Burns* warrants did will not suffice—at least not when "a more specific description of the items subject to seizure could [] reasonably be provided." *Id*. at 776-77.[5] Rather, to satisfy the particularity

[5] *See also*, *e.g.*, *Richardson v. State*, 282 A.3d 98, 120 (Md. 2022) ("Particularity"

requirement, a cell phone warrant's search authorization must be "constrain[ed]" by the scope of the probable cause shown, "'prevent[ing] the seizure of one thing under a warrant describing another,' and avoid[ing] the issuance of search warrants 'on loose, vague[,] or doubtful bases of fact.'" *Id*. at 772 (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927), and *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931)) (first and third alterations in *Burns*). "With a properly particularized warrant, it is the issuing judge who decides 'what is to be taken,' and 'nothing is left to the discretion of the officer executing [it],' making 'general searches . . . impossible.'" *Id*. (quoting *Marron*, 275 U.S. at 196) (alterations in *Burns*).

"A search warrant for data on a modern smart phone . . . must fully comply with the requirements of the Warrant Clause." *Burns*, 235 A.3d at 773. If either the probable cause or the particularity requirement goes unmet, a cell phone search warrant cannot fulfill its constitutional purpose of "ensur[ing] 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) (quoted in *Burns*, 235 A.3d at 772, 775).

So clear and fundamental are the scope of these requirements that this Court held any "'reasonably well trained officer,' reasonably knowledgeable about what the law prohibits," would have known that the warrants at issue in *Burns* were

---

in the context of the Fourth Amendment does not refer to the particular crime(s) under investigation; rather, it refers to the particular "place to be searched, and the persons or things to be seized.") (quoting U.S. CONST. amend. IV).

"'illegal despite the magistrate's authorization,'" even before this Court had addressed probable cause and particularity in the context of a cell phone search. 235 A.3d at 778-79 (quoting *United States v. Leon*, 468 U.S. 897, 922 n.23 (1984)). While the *Burns* warrants authorized an unconstrained search of all cell phone data for "any evidence" of the homicide under investigation, the supporting affidavits only showed probable cause to believe that certain "discrete items" of data would actually relate to the crime. *Id*. at 774. As such, this Court held, they were so obviously overbroad and lacking in particularity that *Leon*'s good faith exception could not save them from the reach of the exclusionary rule. *Id*. at 774, 778-79.

II. THE WARRANT TO SEARCH MR. DEAN'S CELL PHONE FOR "ANY AND ALL EVIDENCE" OF THE HOMICIDE WAS INVALID FOR OVERBREADTH AND LACK OF PARTICULARITY.

Here, as in *Burns*, the warrant application established only probable cause to believe Mr. Dean's cell phone contained a discrete set of text and call log data—all from a 72-hour period—with a nexus to the homicide. Yet the resulting warrant authorized police to search for and seize not only for those texts and call logs, but "[a]ll records on the Device (3/1/2018 – 4/5/2018[)] . . . that relate to" that offense, "including" "[a]ny and all evidence [of] the murder of Tamiya White," plus multiple generic categories of cell phone data as "[e]vidence of user attribution[.]" 2020 Warrant, Attach. B(1)-(2). The one-month restriction on the search authorization was ten times broader than the timeframe of the texts and calls at issue, and it did nothing to restrict the data for which police could search to the only three categories—texts, call logs and (arguably) GPS data—much less the specific digital records for which probable cause was established. The resulting warrant was just as

glaringly overbroad and lacking in particularity as the ones this Court invalidated in *Burns*. Its apparent blessing of authorities' stated intent, in Paragraph 35, to review any and all data on the phone as they saw fit further underscores the warrant's glaring overbreadth and lack of particularity. Indeed, that paragraph alone, as interpreted by the government to authorize the review of literally all data on the phone, R.88 at 5, would render this a general warrant no matter how narrowly the search authorization was tailored.

A. Authorities only showed probable cause for a few items of data.

The warrant affidavit stated that a friend of Mr. Dean's, identified as Witness 2, told police it received from Mr. Dean one incriminating text at 3:59 pm, about an hour before the March 31, 2018 homicide, followed by two incriminating phone calls at 4:16 pm and 5:00 pm, all from a number police confirmed was registered to Mr. Dean. 2020 Warrant, ¶¶ 10-11, 13. Witness 2 further reported that it texted Mr. Dean the next day to ask the name of his girlfriend and received his text in response, "Tamiy [sic] White." *Id*. ¶ 15. Finally, Witness 2 reported that it called Mr. Dean on April 2, 2018 to advise turning himself in. *Id*. ¶ 16. The affidavit indicated that Mr. Dean's cellular phone was seized during his April 5, 2018 arrest, that cellular records obtained by police confirmed his phone was in use "throughout the days before and immediately after the murder," and that those "call detail records" indicated "some call and text data" had not been recovered during a "logical extraction" of the phone's data conducted pursuant to an earlier warrant. 2020 Warrant ¶¶ 26-28.

The affidavit contained no other "'particularized facts' [or] circumstances" to suggest that Mr. Dean's cell phone was used in any other way in connection with the

homicide. *Burns*, 235 A.3d at 772 (quoting *McPhearson*, 469 F.3d at 524). Instead, three boilerplate paragraphs asserted, based on the Detective Rice's "training and experience," the vague and generic claims that:

- "people who commit crime in Washington, D.C. often use their cell phones in ways that reveal their location and/or activities before, after, or while engaging in criminal activity"
- the contents of call logs, text, email and other communication apps "frequently . . . shed light on the cell phone user's location and activity" and on their "relationship with others and its tenor"[6]
- "cell phone[s] recovered from a participant in" "crimes carried out by more than one person" "frequently contain[] evidence of communication among accomplices"
- "a cell phone generally contains" "'user attribution' evidence" such as "electronic communications, lists of contacts and calendar entries, social media account information, and images or video recordings" that "can indicate who has used or controlled the device"
- "a cell phone frequently contains images, video recordings, and audio recordings of the cell-phone user and his close associates" that "may reveal or confirm distinguishing characteristics" that can "help identify them"

2020 Warrant ⁋⁋ 30-32. None of these statements contributes to the probable cause showing for Mr. Dean's phone. To begin, claims based on the affiant's "training and experience" are "wholly conclusory," and give the warrant judge "virtually no basis at all for making a judgment regarding probable cause." *Burns*, 235 A.3d at 772

[6] Detective Rice tacked on, "for example, in the case described above, [the cell phone user's relationship with] the decedent,"—described by Witness 2 as Mr. Dean's girlfriend of four months—"and her family members," 2020 Warrant ⁋⁋ 14, 30, but despite having reviewed Mr. Dean's call detail records, *id*. para. 27, he did not assert any factual basis to conclude that Mr. Dean had used the recovered cell phone to call, text or email with the decedent or her family members.

(quoting *Gates*, 462 U.S. at 239). Even if they had been substantiated, these generic truisms about cell phones "often" or "frequently" containing data that hints at users' activities, movements, and relationships with third parties cannot substitute for the "particularized facts" required to establish a nexus between this homicide and data on *Mr. Dean's* cell phone. *Id*. (citation omitted).[7] To hold otherwise would imply probable cause to search *every* suspect's cell phone, reducing *Riley*'s requirement that police get a warrant before searching arrestees' cell phones from a "meaningful constraint[]" on "'officers[']' unbridled discretion to rummage at will among a person's private effects,'" 573 U.S. at 399 (quoting *Arizona v. Gant*, 556 U.S. 332,

[7] *See also*, *e.g.*, *Commonwealth v. Henley*, 171 N.E.3d 1085, 1109 (Mass. 2021) ("Search warrants relying on the ubiquitous presence of cellular telephones and text messaging in daily life, or generalities that friends or coventurers often use cellular telephones to communicate are insufficient to establish the nexus for a search of such a device.") (internal quotation marks and citation omitted); *Buckham v. State*, 185 A.3d 1, 17 (Del. 2018) ("generalized suspicion[]" that "'criminals often communicate through cellular phones' . . . do[es] not provide a substantial basis to support a probable cause finding") (quoting affidavit); *United States v. Tirado*, No. 16-CR-168, 2018 WL 3245204, at *16-*17 (E.D. Wis. Jan. 26, 2018) ("generic boilerplate statement[s] that 'cellular phones are often used either before, during, or after the commission of crime(s)'" and "'have the potential to show the [suspect's] location'" do not establish probable cause without "specific facts connecting the [phone] and the alleged offense"); *United States v. Ramirez*, 180 F. Supp. 3d 491, 495-96 (W.D. Ky. 2016) (no probable cause to search drug trafficking suspect's cell phone where only "purported nexus" was affiant's "'training and field experience that individuals may keep text messages or other electronic information stored in their cell phones which may relate them to the crime and/or co-defendants/victim'") (quoting affidavit); *In re Search of Certain Cell Phones*, 541 F. Supp. 2d 1, 2 (D.D.C. 2008) (rejecting warrant application when police claimed "narcotic traffickers commonly use cell phones to communicate" without showing how target phones were used in any crime).

345 (2009)), to "little more than a paperwork requirement," *State v. Wilson*, 884 S.E.2d 298, 309 (Ga. 2023) (Pinson, J., concurring).[8]

Beyond their conclusory and generic nature, several of Detective Rice's claims fell short of establishing probable cause for other reasons as well. First, his assertions about cell phone evidence in crimes "carried out by more than one person," 2020 Warrant ¶ 31, did not show probable cause that accomplice communications would be on Mr. Dean's cell phone because the affidavit contained no hint that any accomplices were involved in this offense. Second, there was an insufficient nexus between this offense and the sweeping categories of cell phone data Detective Rice listed as potential "'user attribution' evidence." *Id.* ¶ 32. The phone user's identity was relevant to this investigation only during the times when the two texts and three phone calls were exchanged with Witness 2, and Witness 2's own account that it was communicating with Mr. Dean on those occasions—

[8] *See also*, *e.g.*, *United States v. Opoku*, 556 F. Supp. 3d 633, 641, 644 (S.D. Tex. 2021) (basing warrant solely on "truism that people often communicate plans via cellphones, . . . would undermine . . . *Riley*" and "strike a serious blow to the probable cause requirement"); *Commonwealth v. White*, 59 N.E.3d 369, 376-77 (Mass. 2016) (argument that "'many of those who own a cell phone in effect keep on their person a digital record of nearly every aspect of their lives,' including, presumably, communications with their coventurers" "proves too much" by suggesting "nexus between a suspect's criminal acts and his or her cellular telephone whenever there is probable cause that the suspect was involved in an offense, accompanied by an officer's averment that, given the type of crime under investigation, the device likely would contain evidence. If this were sufficient, . . . it would be a rare case where probable cause to charge someone with a crime would not open the person's cellular telephone to seizure and subsequent search[.]") (brackets, alterations and citation omitted).

including to coordinate a contemporaneous in-person meet up—left no legitimate question that he was the phone's user at the relevant times.[9] *Id.* ¶¶ 10-11. "The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (citation omitted). It does not permit authorities to rummage at will through communications, association data (*e.g.*, contacts and social media), photos and other private information under the guise of looking for cumulative and unnecessary "user attribution" evidence with no meaningful nexus to an investigation. Finally, and for the same reason, the affidavit offered no probable cause for police to mine Mr. Dean's private data for identifying "images, video recordings, and audio recordings" as evidence of this offense. 2020 Warrant ¶ 32. Mr. Dean's identity as the "friend" of "many years" whom Witness Two claimed had confessed the assault was not in any doubt: Witness Two had already identified him by name and photograph, and phone records corroborated that identification. *Id.* ¶¶ 8-16.

What probable cause remains is analogous in scope to that shown in *Burns*.[10]

---

[9] Records listing the phone's number as registered to Mr. Dean, 2020 Warrant ¶ 13, and the fact that Mr. Dean was in possession of the phone three days after the last communication, *id*. ¶ 26, provided further corroboration

[10] While the motions court pointed to the probable cause to arrest Mr. Dean as "differentiat[ing] this case from the *Burns* facts," R.92 at 5, it is a distinction without any meaningful difference. *Burns*'s probable cause determination did not remotely

The application to search Mr. Dean's phone provided a substantial factual basis to believe it would contain evidence of the homicide in the form of two text exchanges with Witness 2 around 3:59 pm on March 31, 2018 and on April 1, 2018; three logged phone calls with Witness 2, around 4:16 pm and 5:00 pm on March 31, 2018, and on April 2, 2018; and, perhaps, GPS data reflecting his location on those dates.[11]

B. The warrant's search authorization lacked particularity and went far beyond the probable cause showing.

A properly particularized warrant would have authorized police to look for

---

turn on his nominal status as a "[w]itness" rather than a suspect at the time of the search. 235 A.3d at 768. Indeed, it was despite ample facts in the warrant affidavit linking Burns to the events surrounding his best friend's murder, *see id*., that this Court held there was no probable cause to search the vast majority of data on his phones. The key fact undergirding that ruling is that the affidavits contained no facts linking *that data* to the murder. *Id*. at 774 ("beyond [certain] discrete items, the affidavits stated no facts that even arguably provided a reason to believe that any other information or data on the phones had any nexus to the investigation"). The Court did not mention *Burns*'s non-suspect status in its overbreadth and particularity discussion because it was irrelevant to the analysis. Indeed, it analogized Burns's case to others invalidating warrants to search suspects' phones. *See id*. at 775-76 (case with "the most closely analogous facts" was one invalidating warrant to search the "chief suspect's" cell phone). Apart from the statement of facts, *Burns* did not mention his non-suspect status at all until *after* it had held the warrants overbroad, insufficiently particular, and too obviously lacking in probable cause for the good faith exception to apply. *Id*. at 775-79. Only then did this Court remark, as icing on the no-good-faith cake, that Burns' non-suspect status made it "*even more* unlikely" the affiant detective could have believed the bulk of the data for which the warrants authorized a search would relate to the homicide. *Id*. at 779 (emphasis added).

[11] Unlike in *Burns*, the warrant affidavit here did not assert Mr. Dean's phone was equipped to log GPS location data. *Compare Burns*, 235 A.3d at 800-801("Based on my training, experience, and research, I know that the Device[] has capabilities that allow it to serve as a . . . GPS navigation device"), *with* 2020 Warrant ⁋ 30 (asserting criminals' cell phones in general "*may* include location information (*e.g.*, GPS data)" without identifying Mr. Dean's phone as GPS enabled) (emphasis added).

those three texts, two call log entries, three days' worth of GPS data, and nothing more. *Burns*, 235 A.3d at 773 (valid "warrant must specify the particular items of evidence to be searched for and seized from the phone and be strictly limited to the time period and information or other data for which probable cause has been properly established"). Such a warrant "easily could have provided a more specific description of the items subject to seizure," *id.* at 777, than "*[a]ll records* on the Device (3/1/2018 – 4/5/2018[)] . . . that relate to the offenses [sic] of murder[.]" 2020 Warrant, Attach. B(1), (1)(a). "The major, overriding problem with [that] description of the object of the search . . . is that the police did not have probable cause to believe that *everything* on the phone" from the arbitrary one-month date range "was evidence of the crime of [murder]." *United States v. Winn*, 79 F. Supp. 3d 904, 919 (S.D. Ill. 2015) (invalidating warrant to search cell phone for "'any or all files' . . . that 'constitute[d] evidence of the offense'") (alteration in *Winn*).

The warrant's overbreadth and lack of particularity were only exacerbated by the literally all-encompassing wish list of evidence "includ[ed]" under Attachment B's "[a]ll records" authorization, *id*., Attach. B(1)(a)-(1)(j),[12] as well as its provision

[12] Beginning with "[a]ny and all evidence related to the murder," the list itemized eight other vague categories of evidence police could only speculate might exist in digital form on the cell phone beyond the few texts and call log entries detailed above (*e.g.*, "[i]nformation relating to Dean's motives and/or intent" or his "possession of a screwdriver," "[a]ny and all evidence related to" his relationships with the decedent and Witness Two) and that, for some categories, lacked the required nexus to this offense (*e.g.*, "[a]ny and all evidence related to Dean's location and/or activities" during undefined "periods of time before and after the Offense," "communications among accomplices," and "the Suspects' [sic] distinguishing characteristics"). 2020 Warrant, Attach. B(1)(a)-(1)(j).

authorizing a search for "logs, phonebooks, saved usernames and passwords, documents, images, and browsing history" as "[e]vidence of user attribution," *Id.*, Attach. B(2).[13] Worse, any constraint imposed by the warrant's anemic restriction to records related to the offense from a one-month date range was obliterated by Paragraph 35's boilerplate "perus[e] all data" clause in the incorporated affidavit. *Id*. ⁋ 35 (emphasis added). That provision explicitly claimed unfettered discretion for authorities to conduct a "'wide-ranging exploratory search[]' not 'carefully tailored to its justifications' — precisely the type of unbridled rummaging 'the Framers intended to prohibit.'" *Burns*, 235 A.3d at 775 (quoting *Garrison*, 480 U.S. at 84); *see also* R.88 at 4-5 (government arguing provision "expressly authorized" authorities to extract and review all data). It is the very definition of a general warrant. *See Steagald v. United States*, 451 U.S. 204, 220 (1981) ("The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to . . . which places should be searched.").[14]

---

[13] Not only was there no probable cause to seek user attribution data as evidence of this particular offense, it is also "constitutionally intolerable for search warrants simply to list generic categories of data typically found on [cell phones] as items subject to seizure." *Burns*, 235 A.3d at 775; *see also People v. Herrera*, 357 P.3d 1227, 1230 (Colo. 2015) (rejecting argument that "any piece of data on the phone" could be sought under warrant for "indicia of ownership" on rationale that all data could be indicative of user, because that would "transform[] the warrant into a general warrant").

[14] Paragraph 35's breathtaking sweep was not remotely justified by the preceding generic, cut-and-paste assertions that "numerous types of user information and metadata" including "images, audio and video recordings, and proximate GPS locations," "are not susceptible to 'word searches' or other narrowly targeted search techniques." 2020 Warrant ⁋ 34. The accuracy of this conclusory claim is uncertain

The grant of such unfettered discretion was especially inexcusable here, where authorities already had a precise accounting from Witness Two and the call detail logs of what type, date and time of data to search in order to find the two texts, three call log entries and GPS data for which there was probable cause. As in *Burns*, "it was readily apparent" that those items "would *not* be found in Mr. [Dean]'s internet search history, photographs, or any of the many other broad categories of data included in the unlimited, template-based search authorized by the warrant[,]" nor in the data from outside the March 1 to April 5 timeframe that Paragraph 35 purported to allow authorities to rummage through anyway. 235 A.3d at 776.

Ultimately, as in *Burns*, this warrant "imposed no meaningful limitations as to how far back in time police could go or what applications they could review and, instead, endorsed the broadest possible search without regard to the facts of the case or the limited showings of probable cause set forth in the affidavits." *Burns*, 235 A.3d at 774-75. It was therefore both overbroad and lacking in particularity in

---

at best. *See*, *e.g.*, Cellebrite, "Release Notes: UFED Physical Analyzer; UFED Logical Analyzer and Cellebrite Reader v7.25" at 3 (Nov. 2019), *available at* https://cellebrite.com/wp-content/uploads/2019/11/ReleaseNotes_UFEDPA-7.25_A4_web.pdf (last accessed Jun. 13, 2023) (explaining users could search for "all location related events surrounding [a] specified address," such as the crime scene, using a graphic map interface.). It also does not even posit that examiners lacked the ability to filter such items by date, as this warrant required. Detective Rice also included a bare assertion that "the complex interrelatedness of cell-phone data" and potential for intentional deception or deletion by "criminals" "may undermine the efficacy of narrow search techniques based on the type, location, or date of information," 2020 Warrant ¶ 34, but he did not elaborate beyond this vague and conclusory claim to explain why or even allege that any of the target information on *Mr. Dean's* phone could reasonably be expected to defy such techniques.

violation of the Fourth Amendment. *Id*. Notwithstanding the one-month restriction—itself overbroad—on the target data, these flaws were at least as glaring here as in *Burns*. The express license for authorities to review *all* data on the phone while searching for that one month's worth of target data further highlighted and underscored these fatal flaws. The warrant was thus "'so lacking in indicia of probable cause'" to search all of that data, and "so facially deficient . . . in failing to particularize the place to be searched [and] the things to be seized . . . that the executing officers [could]not reasonably presume it to be valid." *Leon*, 468 U.S. at 923 (citation omitted); *see also Burns*, 235 A.3d at 779. The trial court erred in denying Mr. Dean's motion to suppress its fruits.

III. THE PROSECUTOR'S RECEIPT OF ALL CONTENT FROM MR. DEAN'S CELL PHONE FLAGRANTLY EXCEEDED THE SCOPE OF THE WARRANT TO SEARCH FOR ONLY ONE MONTH OF RECORDS.

Notwithstanding its obvious and fatal overbreadth, the warrant did impose some limits on what digital records authorities could search for: only those (1) related to the offense that (2) came from a one-month timeframe in 2018. Law enforcement was therefore required to restrain the manner in which it executed the search to what was reasonable in order to find only those target records. Detective Rice and the AUSA brazenly ignored this obligation and instead procured for the AUSA's review a 14,000-page document in which every call log, text, email, photo, app, and other byte of data stored over the life of Mr. Dean's cell phone was translated into and exposed as readable text. This action constituted a search[15] that

[15] *See Arizona v. Hicks*, 480 U.S. 321, 324-25 (1987) (moving stereo to expose serial

dramatically exceeded the authorization to look for evidence from a single one-month timeframe. Thus, even if that time limit and the content restriction to evidence of the offense had been enough to satisfy the probable cause and particularity requirements—and they were not—the search conducted in this case would still have been unlawful.

As the motions court recognized, the search execution here raised a "glar[ing]" concern "that despite the efforts that judges undertook to make sure that the privacy interest of the accused here were [sic] protected in compliance with the Fourth Amendment, the Government ultimately [] seized and received the entire contents of the cell phone" (10/12/21 at 12-13). The AUSA's revelation that "the U.S. Attorney's Office has been doing this in all of its cases" is all the more troubling (10/5/21 at 27). Even though the warrant's obvious invalidity means this Court need not reach Mr. Dean's execution challenge, it should make clear in its opinion that where a warrant is properly particularized—and thus authorizes a search for something less than "all data" related to an offense—handing a full, unfiltered and unredacted copy of a cell phone extraction report to the prosecutor (or any official participating in the investigation or prosecution of the case) is not authorized by Rule 41(e)(2), and will not pass constitutional muster regardless of broad, generic search protocols described in the warrant affidavit.[16]

---

numbers constituted "independent search" because officer took "action . . . which exposed to view concealed portions of the apartment or its contents" being searched, and so "produced [an] additional invasion of respondent's privacy interest").

[16] Although defense counsel "concede[d]" at the suppression hearing, "[f]or the

"[T]he scope of a lawful search is 'defined by the object of the search and the places in which there is probable cause to believe that it may be found." *Garrison*, 480 U.S. at 84. "'Just as ['] probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom,[']probable cause to believe drug trafficking communication may be found in [a] phone's . . . mail application will not support the search of the phone's Angry Birds application.'" *Richardson v. State*, 282 A.3d 98, 118 (Md. 2022) (quoting *In re Nextel Cellular Tel.*, No. 14-MJ-8005-DJW, 2014 WL 2898262, at *13 (D. Kan. June 26, 2014) (quoting *Garrison*, 480 U.S. at 84)). Here, it was plainly unreasonable for the prosecutor to execute a search for one month's worth of data by obtaining the content of every last byte of data, from all dates, on the cell phone.

---

purposes of this discussion," that DFS is "an independent entity" from "law enforcement" (10/5/21 at 20-21), the better view—one espoused by USAO's Forensic Special Counsel Lisa Kreeger-Norman in testimony before the D.C. Council concerning *Brady* disclosures and discovery—is that "in the eyes of the law, the [DFS] laboratory is part of the prosecution team." *See* Video, D.C. Council Committee on the Judiciary & Public Safety Public Hearing on B24-838, the "Restoring Trust and Credibility to Forensic Sciences Amendment Act of 2022," at 4:07:11 – 4:07:18 (June 30, 2022), *available at* https://fb.watch/dZH7dyJRl-/ (last accessed Jun. 15, 2023). Suppression is required in this case regardless of whether the focus is on DFS's action of including in the extraction report all of the cell phone's content from dates *outside* the authorized timeframe, or the detective and AUSA's action in procuring a copy of that report without having it filtered or redacted first. This Court's opinion should make clear, however, that the Fourth Amendment bars DFS from creating and providing to police or AUSAs involved in the investigation or prosecution such an unfiltered extraction report where the warrant includes bright-line temporal or content restrictions on its target records.

This approach was not made necessary by any technological limitation. Although the government alleged below that it is not possible to extract anything less than all data from a cell phone's memory, R.88 at 6-7, that is beside the point. The "physical extraction" of all data is only the first step in a process that next includes parsing the data into readable content and then generating a report organized by data type and date. *See* 10/5/21 at 19-20; 10/26/21 at 200-201. The powerful software DFS utilized in this case enabled the examiner to limit the final report to selected date ranges and categories of data before providing it to the prosecutor, *see supra* n.__, but if it had not, DFS or USAO staff still could have manually redacted or removed pages with content from dates that clearly did not include the target data from March and April 2018, just as the prosecutor prepared a redacted extraction report for trial (10/5/21 at 20).[17] The motions court was thus right to express skepticism "that the Government could not have taken additional steps in some manner to protect the privacy of [Mr. Dean] before the entire extract was transported and given access to the Prosecutor," and to suppress the fruits of this warrant as a result (10/12/21 at 16-17).

It erred, however, in reversing that ruling on the rationale that Superior Court

[17] The AUSA deemed such a "taint team" unworkable due to volume and staffing limitations, since screeners would need familiarity with case facts to "be able to distinguish between what is relevant" in an extraction report (10/5/21 at 32-33). But such knowledge is not required to remove content from dates or data categories outside a specified range. In any event, "if the government cannot create a practical way to perform electronic searches and seizures that does not violate the Fourth Amendment, then it is simply not entitled to that information." *In re Search of Info. Associated with Facebook Acct. Identified by Username Aaron.Alexis*, 21 F. Supp. 3d 1, 9 (D.D.C. 2013) (Facciola, Mag. J.) (hereinafter *Aaron.Alexis*).

Rule of Criminal Procedure 41(e)(2) gives authorities unfettered discretion to "over-seiz[e]" data outside the scope of a digital search warrant. R.92 at 16. Like its "substantially identical . . . federal counterpart," Rule 41(e)(2) merely addresses the logistical impediments to doing forensic examinations of "computers and other electronic storage media . . . during execution of the warrant at the search location," by creating a "two-step process" in which "officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." Sup. Ct. R. Crim. Proc. 41, cmt. to 2017 amendments. The offsite "review" still must be conducted "*consistent with the warrant*." Sup. Ct. R. Crim. Proc. 41(e)(2) (emphasis added). Rule 41(e)(2) thus does not purport to free authorities from a warrant's constraints on what data can be searched for, or where within a digital storage device's memory authorities may search for the target data. Because it was not "consistent with the warrant" to expose to the prosecutor's view all content from all dates on Mr. Dean's cell phone, the execution done here was not authorized by Rule 41(e)(2).

Nor could a rule of procedure authorize the kind of unreasonable search execution at issue here without running afoul of the Fourth Amendment: "[O]verseizure . . . may be reasonable, in light of the practical considerations,"

> But once the Government is able to extract the responsive documents, its right to the overseizure of evidence comes to an end. . . . Once responsive files are segregated or extracted, the retention of non-responsive documents is no longer reasonable . . . [but rather] the equivalent of an unlawful general warrant.

United States v. Ganias, 824 F.3d 199, 232 (2d Cir. 2016) (Chin, J., dissenting); *see also id.* at 218 n.38 (maj. op.) ("We do not disagree with the proposition that the

seizure and retention of computer hard drives or mirrored copies of those drives implicate [privacy] concerns and raise significant Fourth Amendment questions.").

In fact, the very authorities the motions judge cited (R.92 at 15-16) for her recognition that "'over-seizing' is considered to be an 'inherent part of the electronic search process,'" *In re Search of Info. Associated with Facebook Accts. DisruptJ20, lacymacauley, & legba.carrefour*, Nos. 17-CSW-658, -659, -660, 2017 WL 5502809 at *4 (D.C. Super. Ct. Nov. 9, 2017) (Morin, J.) (hereinafter *Facebook Accounts*) (quoting *Aaron.Alexis*, 21 F. Supp. 2d at 8), also warn that such overseizure "often provides the government with 'access to a larger pool of data that it has no probable cause to collect'" *id*. (quoting *Aaron.Alexis*, 21 F. Supp. 3d at 8), and creates "a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant," *id*. (quotation marks and citation omited); *see also*, *e.g.*, *United States v. Comprehensive Drug Testing, Inc.* (*CDT III*), 621 F.3d 1162, 1176 (9th Cir. 2010) (same).

In light of this risk, which arises whenever responsive records are intermingled with nonresponsive ones in physical or digital form, "judicial officials must take care to assure that" their search is "conducted in a manner that minimizes unwarranted intrusions upon privacy." *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976). Mindful of these principles, several courts considering the kind of two-step procedure Rule 41(e)(2) authorizes have rightly concluded that judge-approved search protocols or other minimization procedures are necessary in some if not all cases to "prevent[] the government from overseizing data and then using the process of identifying and segregating seizable electronic data 'to bring constitutionally

protected data into . . . plain view.'" *United States v. Schesso*, 730 F.3d 1040, 1047 (9th Cir. 2013).[18] This warrant's Paragraph 35 claiming authority for law enforcement to "perus[e]" everything on the phone as they saw fit to look for the target records had exactly the opposite effect. This attempt by the government to add a boilerplate inoculation against any challenge to the warrant's execution must fail.

---

[18] *See also*, *e.g.*, *CDT III*, 621 F.3d at 1177 (overseizure "inherent" in "electronic search process" "calls for greater vigilance on the part of judicial officers" to ensure "[t]he process of segregating electronic data that is seizable from that which is not [does] not become a vehicle for the government to gain access to data which it has no probable cause to collect"); *In re Search of Apple iPhone IMEI 01388803738427*, 31 F. Supp. 3d 159, 167-68 (D.D.C. 2014) (hereinafter "*Apple iPhone*") (requiring protocol for "how the government intends to determine where it will search (which "parts"—or blocks—of the iPhone's . . . flash drive)" to "help limit the possibility that locations containing data outside the scope of the warrant will be searched" and ensure "the government is making a genuine effort to limit itself to a particularized search") (citations omitted); *Aaron.Alexis*, 21 F.Supp.3d at 8 (overseizure "would appear to be a *per se* violation of the Fourth Amendment. But due to the current reality that over-seizing is an inherent part of the electronic search process . . . this Court is obliged to create minimization procedures to limit the possibility of abuse by the government.") (internal quotation marks and citation omitted); *Facebook Accounts*, 2017 WL 5502809, at *6-*7 (requiring government to submit minimization protocols prior to search of Facebook data implicating third parties' speech and association rights); *In re Cellular Telephones*, No. 14-MJ-8017-DJW, 2014 WL 7793690, at *8 (D. Kan. Dec. 30, 2014) ("Regarding the place to be searched, . . . in the digital universe, particular information is not accessed through corridors and drawers, but through commands and queries. As a result, in many cases, the only feasible way to specify a particular 'region' of the [device] will be by specifying how to search.") (cleaned up). *See generally In re Search Warrant*, 71 A.3d 1158, 1184 (VT 2012) (limiting what data authorities can search is "essential to meet the particularity requirement of the Fourth Amendment, especially in cases involving record searches where nonresponsive information is intermingled with relevant evidence"); *Richardson*, 282 A.3d at 117 (deeming reasoning of above cases "useful" and "recommend[ing] that issuing judges in Maryland consider including search protocols in cell phone search warrants in appropriate cases").

Because the prosecutor's seizure of all cell phone data translated into readable format "flagrantly exceed[ed] the scope of the warrant," the fruits of that seizure should be suppressed. *Lewis*, 147 A.3d at 245 ("if officers executing a search warrant . . . flagrantly exceed the scope of the warrant, all of the evidence seized may be subject to suppression); *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) ("[g]overnment agents 'flagrantly disregard' the terms of a warrant so that wholesale suppression is required [] when (1) they effect a widespread seizure of items that were not within the scope of the warrant, and (2) do not act in good faith." (internal quotation marks and citations omitted).[19]

[19] Although a lack of good faith may be required to show "flagrant disregard" justifying the suppression of all fruits, *Shi Yan Liu*, 239 F.3d at 141, the *Leon* good faith exception—which turns on an officer's mistaken but reasonable reliance on the validity of a search authorization—should not otherwise apply to execution challenges, where officers have searched beyond what a warrant authorizes. *See United States v. Angelos*, 433 F.3d 738, 746 (10th Cir. 2006) ("we have held that '[t]he *Leon* good faith exception will not save an improperly executed warrant'") (citation omitted). *Cf. United States v. Pimentel*, 26 F.4th 86, 91-92 (1st Cir. 2022) (while "[w]e have not bypassed the inquiry into good faith altogether" in execution challenges, "the good-faith exception only saves searches 'that it was reasonable to believe were covered by the warrant'") (citation omitted).

Respectfully submitted,

s/Fleming Terrell
Samia Fam, Bar No. 394 445
Fleming Terrell, Bar No. 998 774

PUBLIC DEFENDER SERVICE
FOR THE DISTRICT OF COLUMBIA*
633 Indiana Avenue, NW
Washington, DC 20004
(202) 628-1200

District of Columbia
Court of Appeals

REDACTION CERTIFICATE DISCLOSURE FORM

Pursuant to Administrative Order No. M-274-21 (filed April 3, 2023), this certificate must be filed in conjunction with all briefs submitted in all criminal cases designated with a "CF" (criminal felony), "CM" (criminal misdemeanor), "CT" (criminal traffic), and "CO" (criminal other) docketing number. Please note that although briefs with above designations must comply with the requirements of this redaction certificate, criminal sub-case types involving child sex abuse, cruelty to children, domestic violence, sexual abuse, and misdemeanor sexual abuse will not be available for viewing online.

If you are incarcerated, are not represented by an attorney (also called being "pro se"), and not able to redact your brief, please initial the box below at "G" to certify you are unable to file a redacted brief. Once Box "G" is checked, you do not need a file a separate motion to request leave to file an unredacted brief.

I certify that I have reviewed the guidelines outlined in Administrative Order No. M-274-21, filed April 3, 2023, and Super. Ct. Crim. R. 49.1, and removed the following information from my brief:

A. All information listed in Super. Ct. Crim. R. 49.1(a) has been removed, including:

(1) An individual's social-security number
(2) Taxpayer-identification number
(3) Driver's license or non-driver's' license identification card number
(4) Birth date
(5) The name of an individual known to be a minor as defined under D.C. Code § 16-2301(3)
(6) Financial account numbers

(7) The party or nonparty making the filing shall include the following:

(a) the acronym "SS#" where the individual's social-security number would have been included;
(b) the acronym "TID#" where the individual's taxpayer-identification number would have been included;
(c) the acronym "DL#" or "NDL#" where the individual's driver's license or non-driver's license identification card number would have been included;
(d) the year of the individual's birth;
(e) the minor's initials;
(f) the last four digits of the financial-account number; and
(g) the city and state of the home address.

B. Any information revealing the identity of an individual receiving or under evaluation for substance-use-disorder services.

C. All pre-sentence reports (PSRs); these reports were filed as separate documents and not attached to the brief as an appendix.

D. Information about protection orders, restraining orders, and injunctions that "would be likely to publicly reveal the identity or location of the protected party," 18 U.S.C. § 2265(d)(3) (prohibiting public disclosure on the internet of such information); *see also* 18 U.S.C. § 2266(5) (defining "protection order" to include, among other things, civil and criminal orders for the purpose of preventing violent or threatening acts, harassment, sexual violence, contact, communication, or proximity) (both provisions attached).

E. Any names of victims of sexual offenses except the brief may use initials when referring to victims of sexual offenses.

F. Any other information required by law to be kept confidential or protected from public disclosure.

Initial here

G. I certify that I am incarcerated, I am not represented by an attorney (also called being "pro se"), and I am not able to redact this brief. This form will be attached to the original filing as record of this notice and the filing will be unavailable for viewing through online public access.

Fleming Terrell
Signature

22-CF-0447
Case Number(s)

Fleming Terrell
Name

June 20, 2023
Date

fterrell@pdsdc.org
Email Address

CERTIFICATE OF SERVICE

I hereby certify that corrected copies of the foregoing brief have been served electronically upon Chrisellen Kolb, Esq., Chief, Appellate Division, Office of the United States Attorney, 555 Fourth Street, NW, Room 8104, Washington, D.C. 20530, and upon counsel for Appellant, Anne K. Walton, Esq., 455 Massachusetts Avenue, NW, Suite 347, Washington, D.C. 20001, this 20th day of June, 2023.

s/Fleming Terrell
Fleming Terrell