UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
	:	
- v -	:	**18 Cr. 363 (RJS)**
	:	
WILFREDO SEPULVEDA,	:	
a/k/a "Dionicio De La Cruz Rodriguez,"	:	
Defendant.	:	

DEFENDANT WILFREDO SEPULVEDA'S MOTION TO SUPPRESS EVIDENCE

Federal Defenders of New York
Attorneys for Defendant
52 Duane Street - 10th Floor
New York, NY 10007
Tel.: (212) 417-8749

Clay H. Kaminsky
Of Counsel

TO: GEOFFREY BERMAN
United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, NY 10007
Attn: AUSA Kyle Wirshba

TABLE OF CONTENTS

NOTICE OF MOTION

Defendant Wilfredo Sepulveda a/k/a Dionicio De La Cruz Rodriguez hereby moves this Court, pursuant to Rule 12 of the Federal Rules of Criminal Procedure, for an order suppressing all evidence obtained from the unconstitutional search of his cell phones.[1] In the alternative, he asks this Court to set this motion for an evidentiary hearing. The warrant authorizing the search of Mr. Sepulveda's phones was unsupported by probable cause, overbroad, and unparticularized, and the government's search and seizure of Mr. Sepulveda's personal data was unrestricted.

FACTUAL BACKGROUND

Mr. Sepulveda was arrested in connection with this case on May 14, 2018, near the intersection of East 202nd Street and Briggs Avenue in the Bronx. In his possession were two cellular telephones: a white iPhone 7 and a black LG flip phone.

On May 15, 2018, Mr. Sepulveda was presented—by video conference, from Jacobi Medical Center—before Magistrate Judge Barbara Moses on a Complaint sworn out by ATF agent Tyler S. Miceli. The three-count Complaint alleged that Mr. Sepulveda had robbed a narcotics stash house with a gun just prior to his arrest, in violation of [1] 18 U.S.C.§ 1951; [2] 21 U.S.C. §841(a)(1), (b)(1)(B); and

[1] At the August 9, 2018 conference in this matter, Mr. Sepulveda informed the Court of his intention also to move for suppression of a post-arrest statement taken from him in the emergency room of Jacobi Medical Center. The government subsequently provided notice that it does not intend to use that statement at trial. In an abundance of caution, Mr. Sepulveda informs the Court that this statement was taken in violation of Miranda and was also made involuntarily under the Fifth Amendment.

[3] 18 U.S.C. § 924(c)(1)(A)(ii). A grand jury returned a three-count indictment charging Mr. Sepulveda with the same offenses a week later, on May 22, 2018.

On June 4, 2018, Agent Miceli made an application in this District to Magistrate Judge Robert W. Lehrburger for a warrant to search Mr. Sepulveda's phones. See **Exhibit A** (Warrant Application & Supporting Affidavit). In his supporting affidavit, Agent Miceli recounted with specificity why he believed there was probable cause that Mr. Sepulveda committed an uncharged robbery on February 9, 2018 and the charged May 14, 2018 robbery. See Ex. A ¶¶ 7–8.

But when it came to probable cause for searching Mr. Sepulveda's phones, Agent Miceli ran out of specifics. Instead, he relied on the generality that everyone in today's society uses cell phones for everything:

> *Like individuals engaged in any other kind of activity*, individuals who engage in drug distribution store records relating to their activity and to persons involved with them in that activity on electronic devices such as the Subject Devices. . . .
>
> Likewise, *like individuals engaged in any other kind of group activity*, individuals who engage in robberies use their phones to plan, coordinate, and follow-up with others involved in the activity.

Id. ¶¶ 9–10 (emphasis added).

Regarding the iPhone, Agent Miceli wrote "video from the lobby of the building containing Apartment-1 depicts RODRIGUEZ using what appears to be an iPhone. Similarly, video from the apartment building where RODRIGUEZ dressed himself in the wig and dress depicts RODRIGUEZ using The iPhone's camera to look at himself. In the video, RODRIGUEZ stares at The iPhone's screen, repeatedly adjusting his wig and clothing." Id. ¶ 11

Regarding the flip phone, Agent Miceli wrote "based on my training and experience, I also know that individuals involved in drug trafficking, use multiple phones. In particular, individuals involved in drug trafficking will maintain a cheaper phone that can be easily and often thrown out and replaced, also known as a 'burner phone.' Because drug traffickers do not wish to throw away expensive phones, such as The iPhone, they will buy and maintain different burner phones for short periods. The Flip Phone is the type of phone that drug traffickers will purchase as a burner phone to be used for a short period." Id. ¶ 12

There is no allegation in the warrant affidavit that Mr. Sepulveda used either phone to make any call; keep any contacts; receive any voicemail; send any text, chat, or email; or to take any photograph or video; keep any calendar; nor store any bank records in connection with any identified offense. Yet Agent Miceli sought the following categories of evidence from the phone, which he enumerated in Attachment A:

1. the phone number associated with the Subject Device;
2. address books and contact lists;
3. log information of phone numbers of incoming and outgoing calls;
4. other caller-identification information, including names, phone numbers, and addresses;
5. opened and unopened voicemail messages;
6. text, data, chat, digital photographs and video, MMS (i.e., multimedia messaging service), and SMS (i.e., short message service), email messages (collectively, "text messages"), any attachments to those text messages, such as digital photographs and videos, and any associated information, such as the phone number from which the text message was sent, pertaining to the robberies, the location of the robberies, the

occupants of the robbed apartments, narcotics, and narcotics trafficking,

7. calendar or other scheduling information;

8. bank records, checks, credit card bills, account information, and other financial records;

9. Evidence of user attribution showing who used or owned the Subject Device at the time the records and items described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

Ex. A, Attachment A.

According to Agent Miceli's affidavit, law enforcement personnel planned to review the electronically stored information ("ESI") "sent, received, or obtained from the period of February 1, 2018 to May 23, 2018 on the Subject Devices for information responsive to the warrant." Ex. A at 8. Agent Miceli listed some examples of the "various techniques" that law enforcement may use to conduct the review, including "conducting a file-by-file review by 'opening' or reading the first few 'page' of such files." Id. He wrote that "[l]aw enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant." Id. at 9. But, "depending on the circumstances," he wrote, "law enforcement may need to conduct a complete review of all the ESI from the Subject Device to locate all data response to the warrant." Id.

The search warrant issued the same day, June 4, 2018. See **Exhibit B** (Search Warrant). The warrant incorporates Attachment A, listing all of the categories of ESI sought. It does not incorporate Agent Miceli's affidavit.

On about July 12, 2018, the government produced in discovery a complete logical and file system extraction of the flip phone in Cellebrite UFED format. On about August 6, 2018, it produced a complete logical and physical extraction of the iPhone in Cellebrite UFED format. If any effort had been made by the government to limit its review of the ESI on these devices, it was not apparent.

LEGAL STANDARDS

While law enforcement agents have long been permitted to search the person of a defendant incident to a lawful arrest for whatever evidence they may find of his offense, a warrant is required to search a cell phone, "even when a cell phone is seized incident to arrest." See Riley v. California, 134 S. Ct. 2473, 2482, 2493 (2014). The Supreme Court has reasoned that, because of the vast array of data that individuals can and do store on their cell phones, "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house. A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form." Id. at 2491. "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions[.]" Id. at 2489. The Court extended this logic to both "smart phones" and "flip phones." Id. at 2480–81.

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend.

IV. The Fourth Amendment was adopted largely to "prevent . . . 'general, exploratory rummaging in a person's belongings' and the attendant privacy violations." United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)).

"[A] warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." Kentucky v. King, 563 U.S. 452, 459 (2011). In addition to ensuring that there is probable cause to seize and search a cell phone, courts must also give special attention to whether a warrant to search a cell phone is impermissibly overbroad. A search warrant is overbroad in violation of the Fourth Amendment if its "description of the objects to be seized is . . . broader than can be justified by the probable cause upon which the warrant is based." Galpin, 720 F.3d at 446. A warrant that purports to "authorize the seizure of, essentially, all documents" exceeds the scope of probable cause. United States v. Wey, 256 F. Supp. 3d 355, 393 (S.D.N.Y. 2017).

"The particularity requirement has three components. First, a warrant must identify the specific offense for which the police have established probable cause. Second, a warrant must describe the place to be searched. Third, the warrant must specify the items to be seized by their relation to designated crimes." Galpin, 720 F.3d at 445-46 (internal citations omitted). The particularity requirement "'makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the

discretion of the officer executing the warrant.'" Id. at 446 (quoting Marron v. United States, 275 U.S. 192, 196 (1927)).

Suppression is the appropriate remedy where the affidavit submitted in support of a search warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable" or 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. Leon, 468 U.S. 897, 923, (1984) (internal quotation marks omitted). Suppression is required of evidence outside the scope of a warrant that is searched or seized. See United States v. Matias, 836 F.2d 744, 747 (2d Cir. 1988). Where agents flagrantly disregard the terms of a warrant and effect the "widespread seizure of items that were not within the scope of the warrant," blanket suppression of all evidence obtained by the search may be appropriate. United States v. Liu, 239 F.3d 138, 140–142 (2d Cir. 2000) (explaining that "[t]he rationale for blanket suppression is that a search that greatly exceeds the bounds of a warrant and is not conducted in good faith is essentially indistinguishable from a general search.")

ARGUMENT

The government's search of Mr. Sepulveda's cell phones violated the Fourth Amendment. First, the government lacked probable cause to search Mr. Sepulveda's phones; at a minimum the search warrant that it obtained is overbroad because it covers far more data than could possibly be justified. Second, the warrant fails particularity; it does not sufficiently specify the items to be seized by

their relation to designated crimes. Third, the search likely exceeded even the broad scope of the warrant. Therefore all evidence derived from the unconstitutional search of Mr. Sepulveda's phones should be suppressed.

1. The phone warrant is not supported by probable cause.

Mr. Sepulveda was arrested upon probable cause to believe that he committed a stash house robbery. But cell phones cannot be searched incident to a lawful arrest; separate probable cause to search is required. Riley v. California, 134 S Ct. 2473, 2493 (2014). "[A] determination of probable cause to search is not the same as a determination that there is, at the same time, probable cause to arrest, or vice versa." United States v. Pabon, 871 F.3d 164, 181 (2d Cir. 2017); United States v. Burton, 288 F.3d 91, 103 (3d Cir. 2002) ("[P]robable cause to arrest does not automatically provide probable cause to search the arrestee's home."); United States v. Santarsiero, 566 F. Supp. 536, 538 (S.D.N.Y. 1983) ("Probable cause to arrest an individual does not, in and of itself, provide probable cause to search that person's home or car."). Rather, probable cause to search must be based on "a sufficient nexus between the criminal activities alleged" and the location or items searched. United States v. Singh, 390 F.3d 168, 182 (2d Cir. 2004). In particular, searches must be supported by probable cause showing that there is a "fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983).

Agent Miceli's affidavit fails to establish a sufficient nexus between the criminal activities alleged and Mr. Sepulveda's phones to demonstrate a fair probability that contraband or evidence of a crime will be found on them. In an age

when cell phones are so pervasive that they might be mistaken for "an important feature of human anatomy," Riley, 134 S. Ct. at 2484, merely possessing a phone cannot be sufficient cause to search it. Moreover, it is increasingly common for individuals to have more than one phone.[2]

There is no indication in the warrant affidavit that Mr. Sepulveda used a phone for criminal activity. Instead, the warrant affidavit attempts to establish probable cause by faulty syllogism—that Mr. Sepulveda is engaged in crime so, "[l]ike individuals engaged in any other kind of activity," he must have used his phones to engage in that activity. See Ex. A ¶ 9. This line of reasoning—that people use their phones for many activities, so a criminal suspect likely used his phone in his alleged criminal activities—is an attempt to end-run Riley. By Agent Miceli's logic, the phone of any arrestee would be subject to search on the basis that it may have been used in the offense of arrest. That is not the law. A cell phone is not contraband or inherently suspicious. There must be probable cause to believe that the device contains evidence of a crime.

At its most specific, the affidavit states that there is video footage of Mr. Sepulveda holding what appears to be an iPhone, staring at his iPhone's screen, and adjusting his wig and clothing before the May 14 incident. Ex. A ¶ 11. This falls far

[2] Worldwide 12% of mobile users had multiple devices had multiple mobile devices in 2012, with that number projected to increase to 25% by 2016. The State of Broadband 2012: Achieving Digital Inclusion for All, The Broadband Commission for Digital Development, 16 (2012), http://www.broadbandcommission.org/Documents/bb-annualreport2012.pdf. According to data from the World Bank, in the United States for every 100 people there are roughly 123 cellular device subscriptions, indicating a high number of individuals with multiple cellular subscriptions. Mobile Cellular Subscriptions (Per 100 People), The World Bank Data (last visited Sept. 10, 2018), https://data.worldbank.org/indicator/IT.CEL.SETS.P2?end=2016&start=2016&view=map. In an age "when work and home lives are more intertwined than ever, there's a slice of the population opting to maintaining the divide by carrying two phones." Elizabeth Holmes, People for Whom One Cellphone Isn't Enough, The Wall Street Journal (April 1, 2014, 7:12pm), https://www.wsj.com/articles/people-who-use-two-cellphones-1396393393.

short of establishing that any evidence of criminal activity would be found on Mr. Sepulveda's phone. The only "use" he is alleged to have made of the phone is essentially as a mirror to adjust his clothing. It is highly unlikely that that this alleged use of the phone resulted in the creation of any ESI, since people who use their phone's camera to look at themselves rarely record video as they do so.

If there were probable cause to search—and there is not—it would be limited to a search of Mr. Sepulveda's iPhone for a video of himself dressing on May 14, 2018. Accordingly, the warrant is grossly overbroad.

2. The warrant lacks particularity.

The warrant to search Mr. Sepulveda's phones not only lacks probable cause; it is also a general warrant that lacks the specificity required for any kind of tailored search. The warrant lays out nine broad categories of ESI sought by law enforcement. While this enumeration may appear to limit the scope of the warrant, in reality it comprehensively lists almost all of the imaginable data that can be stored on a cell phone.

The particularity requirement "is necessarily tied to the . . . probable cause requirement." In re 650 Fifth Ave. & Related Props., 830 F.3d 66, 98 (2d Cir. 2016). That is because " '[b]y limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.'" Id. (quoting Maryland v. Garrison, 480 U.S. 79, 84 (1987)).

But the warrant here authorizes the government to search for information with no articulated connection to the factual allegations in the affidavit, including "address books," "contact lists," "log information of phone numbers of incoming and outgoing calls," "other caller identification information," "opened and unopened voicemail messages," "calendar and other scheduling information," "bank records, checks, credit card bills, account information, and other financial records," and, as a catchall, "evidence of user attribution showing who used or owned" the phones. Ex. B, Attachment A. Taken collectively, the enumerated categories represent an extremely broad swath of personal information with no discernable connection to the discrete robberies at issue in this case.

Even individually, many of the categories are impermissibly overbroad, describing generic types of data without any reference to the suspected criminal conduct. See United States v. Wey, 256 F.Supp.3d 355, 385 (S.D.N.Y. 2017) (finding a warrant lacked particularity where it set forth "expansive categories of often generic items subject to seizure—several of a 'catch-all' variety—without, crucially, any linkage to the suspected criminal activity"). For instance, warrants for "checks, cash and other financial instruments" and "calendars and patient appointment records" have been deemed overbroad when the warrant failed to specify to whom those records might relate. United States v. Zemlyansky, 945 F. Supp. 2d 438, 457-58 (S.D.N.Y. 2013). Those defective warrants mirror the instant warrant, which requests bank records and calendar information without specifying to whom that information might relate.

The only category that appears to have any cognizable limitation is category 6:

> text, data, chat, digital photographs and video, MMS (i.e., multimedia messaging service), and SMS (i.e., short message service), email messages (collectively, "text messages"), any attachments to those text messages, such as digital photographs and videos, and any associated information, such as the phone number from which the text message was sent, *pertaining to the robberies, the location of the robberies, the occupants of the robbed apartments, narcotics, and narcotics trafficking*,

Id. (emphasis added). But nowhere does the warrant describe these robberies, identify the locations where they occurred, or name the occupants of the robbed apartments. Indeed, this is the only reference to the alleged facts in the warrant and accompanying attachment. Without context, these words lack content. They also provide insufficient guidance to the wide array of law enforcement personnel responsible for executing the warrant. See Ex. B, Attachment A (including "attorney support staff, agency personnel assisting the government . . ., and outside technical experts"). Consequently, the warrant lacks sufficient particularity under the Fourth Amendment. See United States v. Galpin, 720 F.3d 436, 446 (2d Cir. 2013) ("'As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.'") (quoting Marron v. United States, 275 U.S. 192, 196 (1927)).

Agent Miceli does provide additional facts related to the robberies in his affidavit in support of the warrant application. However, Agent Miceli's affidavit is not incorporated into the warrant. See Groh v. Ramirez, 540 U.S. 551, 557, (2004); 650 Fifth Ave. 830 F.3d at 99–100 ("In Groh, the Supreme Court stated that the Fourth Amendment's particularity requirements must be satisfied 'in the warrant,

not in the supporting documents.'"). Here, as in Groh, there is no "deliberate and unequivocal" language that incorporates the affidavit into the warrant. 650 Fifth Ave., 830 F.3d at 100. There is no explicit incorporating clause, and there is no implicit reference to an affidavit or second attachment. As a result, the affidavit cannot "cure an otherwise defective search warrant." United States v. Rosa, 626 F.3d. 56, 64 (2d Cir. 2010); see also Wey, 256 F.Supp.3d at 384.

Because Agent Miceli's affidavit is not incorporated into the warrant, the warrant also lacks any temporal limitation on the files for which the government may search. Cf. Ex. A at 8 (stating in the affidavit that agents would limit their search to the period from February 1, 2018 to May 23, 2018). Absent a date range, the warrant authorizes a nearly boundless search of personal data on two devices. Such an open-ended intrusion is unsupported by probable cause, constitutionally overbroad, and devoid of the particularity demanded by the Fourth Amendment. See, e.g., Wey, 256 F. Supp. 3d at 387 (finding warrant lacked particularity for failing to include a date range, despite "rather precise timeframes" identified in an unincorporated affidavit); United States v. Levy, 2013 WL 664712, at *11 n.7 (S.D.N.Y. Feb. 25, 2013) ("Several courts in this Circuit have recognized the constitutional questions that are raised by the lack of a specific date range in a warrant for documentary records and warned the Government to include one when possible.") (citing cases), aff'd, 803 F.3d 120 (2d Cir. 2015).

Like other warrants for digital data that have been deemed defective, the warrant to search Mr. Sepulveda's phones "lacks the requisite specificity to allow

for a tailored search of [the defendant's] electronic media" and "fails to link the items to be searched and seized to the suspected criminal activity." Rosa, 626 F.3d at 62; see also Galpin, 720 F.3d at 447 (warrant to search electronics for "evidence of violations of NYS Penal Law or Federal Statutes" violated particularity requirement); United States v. Winn, 79 F. Supp. 3d 904. 920 (S.D. Ill. 2015) (warrant to search a cell phone "was overbroad, because it allowed the police to search for and seize broad swaths of data without probable cause to believe it constituted evidence of [the offense].").

The Second Circuit has noted that digital searches "demand[] a heightened sensitivity to the particularity requirement" due to the "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." Galpin, 720 F.3d at 447 (quoting United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010) (quotation marks omitted)). A general phone warrant—based on nothing more than the fact of Mr. Sepulveda's arrest and the charges against him—is precisely what the government sought and obtained in this case.

The warrant leaves much to the discretion of the searching officers. Instead of providing officers with discrete pieces of data to search for, it gives officers only a vague and unsubstantiated hint that Mr. Sepulveda may have used his phone to engage in the activities of drug distribution or robbery. The warrant affidavit states that the search for this information would be "analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain

pertinent files" and "performing a cursory examination of each document in a file cabinet to determine its relevance." See Ex. A at 8. However, because the officers are given so little information as to what information might be relevant, the search described by the warrant would by necessity be far more than cursory. As the Second Circuit noted, while police could not "search for false tax documents by viewing the suspect's home video collection," "[s]uch limitations are largely absent in the digital realm, where the size or other outwardly visible characteristics of a file may disclose nothing about its content." Galpin, 720 F.3d at 447.

Because the warrant fails to describe the items to be seized and their relation to the offense with particularity, it is facially defective.

3. The search and seizure likely exceeded the scope of the warrant.

Finally, the government appears to have seized the entire contents of Mr. Sepulveda's two cell phones using a forensic extraction tool manufactured by Cellebrite, a private company. Cellebrite makes a Universal Forensics Extraction Device ("UFED") that can "extract and decode every ounce of data" on a cell phone.[3] That is exactly what the government did here; it copied every bit of data on Mr. Sepulveda's phones. This much is clear from the two complete copies of Mr. Sepulveda's devices provided to defense counsel using the Cellebrite software format. The Cellebrite report indicates that the government performed full logical extractions on both devices, a full file system extraction the flip phone, and a full

[3] See, e.g., Cellebrite, UFED Ultimate (2018), available at https://www.cellebrite.com/en/products/ufed-ultimate/.

physical extraction on the iPhone, including deleted files and categories of data even beyond the terms of an already overbroad warrant.

In its warrant application, the government pledged to "make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant." Ex. A at 9. But there is no indication that the government made any effort to do so. There is no evidence that technicians imposed any date restriction on the data they searched and seized. Nor is there any evidence that they used a search protocol or keyword searches to limit their review of Mr. Sepulveda's personal data to focus on information responsive to the warrant. Indeed, it is not apparent that they had read or received a copy of Agent Miceli's unincorporated affidavit, let alone followed the procedures it describes.

What is apparent is that the seizure was all-encompassing. There appears to have been no effort at all to narrow the scope of the data searched and seized—in either deliberate or reckless disregard of the terms of the warrant and the representations the government made in its application and affidavit. Therefore, the indiscriminate search and seizure of Mr. Sepulveda's data was contrary to the Fourth Amendment and should be suppressed in their entirety.

In the event the Court declines to suppress all evidence obtained pursuant to this facially defective warrant, a hearing is necessary to fully determine the Fourth Amendment issues raised by this motion. In particular, it is critical to the defense to determine how the government actually conducted its search and seizure of Mr. Sepulveda's cell phones. A hearing is necessary to assess whether the government

complied with the process for searching ESI outlined in the warrant, and if so, which available techniques were employed. A hearing is also necessary to assess whether the government complied with its representations in the warrant affidavit, and if so, how they tailored their search to satisfy the Fourth Amendment's particularity requirement.

CONCLUSION

For the reasons stated, the Court should grant this motion to suppress evidence or, in the alternative, hold an evidentiary hearing.

Dated: September 10, 2018

Respectfully submitted,
Federal Defenders of New York

By: /s/
Clay H. Kaminsky
Attorneys for Defendant
52 Duane Street - 10th Floor
New York, New York 10007
Tel.: (212) 417-8749

EXHIBIT A

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

(1) a White Model A1661 iPhone 7 Plus bearing IC 579C-E3087A; and (2) a black LG flip phone bearing serial number 707VTEY100124 and IMEI number 359926-08-100124-3

Case No. 18 MAG . 4774

APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attached Affidavit and Attachment A

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)	*Offense Description(s)*
18 USC 1951, 924(c); 21 USC 812, 841	Title 18, United States Code, Section 1951 (Hobbs Act robbery); Title 21, United States Code, Sections 812, 841 (narcotics possession with intent to distribute); Title 18, United States Code, Section 924(c) (use of a firearm in connections with a crime of violence or narcotics trafficking offense)

The application is based on these facts:

See Attached Affidavit and its Attachment A

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Tyler S. Miceli, Special Agent, ATF
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/4/2018

Judge's signature

City and state: New York, NY

The Honorable Robert W. Lehrburger, U.S.M.J.
Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for (1) a White Model A1661 iPhone 7 Plus bearing IC 579C-E3087A; and (2) a black LG flip phone bearing serial number 707VTEY100124 and IMEI number 359926-08-100124-3.

TO BE FILED UNDER SEAL

Agent Affidavit in Support of Application for Search and Seizure Warrant

SOUTHERN DISTRICT OF NEW YORK) ss.:

Tyler S. Miceli, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I have been a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF") for approximately 3 years. For approximately 1 year, I have been assigned to the Joint Robbery Task Force. During my time assigned to the Joint Robbery Task Force, I have investigated many robberies, including robberies that target narcotics and narcotics proceeds. I have also participated in the execution of search warrants involving electronic evidence.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic devices specified below (the "Subject Devices") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and

conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Devices

3. The Subject Devices are particularly described as (1) a White Model A1661 iPhone 7 Plus bearing IC 579C-E3087A (the "The iPhone"); and (2) a black LG flip phone bearing serial number 707VTEY100124 and IMEI number 359926-08-100124-3 (the "Flip Phone").

4. Based on my training, experience, and research, I know that The iPhone has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In addition, I know that the Flip Phone has capabilities that allow it to serve as a wireless telephone, digital camera, and PDA.

5. The Subject Devices are presently located in the Southern District of New York.

C. The Subject Offenses

6. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Devices contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1951 (Hobbs Act robbery); Title 21, United States Code, Sections 812, 841 (narcotics possession with intent to distribute); Title 18, United States Code, Section 924(c) (use of a firearm in connections with a crime of violence or narcotics trafficking offense) (the "Subject Offenses ").

II. Probable Cause

A. Probable Cause Regarding Subjects' Commission of the Subject Offenses

7. I believe there is probable cause that, on February 9, 2018, DIONICIO DE LA CRUZ RODRIGUEZ (the "Target Subject" or "RODRIGUEZ"), along with two coconspirators, ("CC-1," "CC-2," and collectively, the "Coconspirators") committed a home invasion robbery.

a. Dressed as painters, the Coconspirators waited in the hallway of an apartment building in the Bronx, just outside a particular apartment ("Apartment-1"). When the resident of Apartment-1 came home ("Victim-1"), the Coconspirators brandished a firearm and pushed their way into Apartment-1.

b. Once inside, the Coconspirators demanded money and, when Victim-1 provided only a small amount, one of the Coconspirators stated, in substance and in part, "We ain't looking for small amounts" [sic]. The Coconspirators proceeded to burn both of Victim-1's cheeks with a hot iron and poke Victim-1 on the left side of his face with a knife. Vicitm-1 provided all of the cash in Apartment-1.

c. Subsequent investigation uncovered video footage depicting RODRIGUEZ in the lobby of the building in which Apartment-1 is located. In addition, DNA found on the knife used during the robbery matched RODRIGUEZ's DNA profile maintained on a law enforcement database.

8. I believe there is probable cause that, on or about May 14, 2018, RODRIGUEZ, committed another home invasion robbery.

a. That day, RODRIGUEZ entered an apartment building in the Bronx and disguised himself in a wig and women's dress.

b. Shortly thereafter, at approximately 11:00 am, RODRIGUEZ disguised in the wig and dress, entered into a neighboring apartment building in the Bronx, New York and entered a particular apartment ("Apartment-2") whose sole occupant was an 83-year old woman ("Victim-2").

c. After he gained entry to Apartment-2, RODRIGUEZ brandished a knife and demanded that Victim-2 enter her bedroom and stay there. RODRIGUEZ then began rummaging through the remaining rooms in Apartment-2.

d. At some point during the robbery, another resident of the apartment building ("Witness 1") knocked on the door of Apartment-2. When he did so, Witness-1 observed through Apartment-2's peephole an individual later identified as RODRIGUEZ dressed in a wig and dress. Witness-1 then returned to his home to alert the family of Victim 1 about what he had observed.

e. RODRIGUEZ eventually found inside Apartment-2 cash and approximately three kilograms of mixtures and substances that I believe contain narcotics, based on their appearance, the nature of their packaging, and lab results from other items inside the home. RODRIGUEZ placed the drugs and cash into a pillowcase (the "Pillowcase") and fled Apartment-2.

f. Carrying the Pillowcase, RODRIGUEZ left the apartment building. As RODRIGUEZ did so, however, Witness-1 saw RODRIGUEZ leaving and pursued him on foot. When Witness-1 caught up to RODRIGUEZ, RODRIGUEZ brandished a firearm, which Witness-1 managed to wrestle away. In the ensuing altercation, RODRIGUEZ bit Witness-1 on the left forearm, right bicep, and finger, causing lacerations and bleeding. Also during the altercation, RODRIGUEZ told Witness-1, in sum and substance, that Witness-1 could take a kilo from the Pillowcase if Witness-1 ended the altercation.

g. Shortly thereafter, officers of the New York City Police Department ("NYPD") arrived at the scene and ended the altercation between RODRIGUEZ and Witness-1. Officers also recovered from the scene The iPhone, the firearm brandished by RODRIGUEZ, the Pillowcase containing $13,000 in cash and approximately three kilograms of mixtures and substances that I

believe contain narcotics, the knife RODRIGUEZ brandished in Apartment-2, and the wig and dress worn by RODRIGUEZ.

h. Officers placed RODRIGUEZ under arrest and brought Victim-2 to the scene. Victim-2 identified RODRIGUEZ as the perpetrator of the robbery. NYPD then transported RODRIGUEZ to a hospital in the Bronx.

i. On May 15, 2018, while RODRIGUEZ was still in the hospital, RODRIGUEZ was charged by criminal complaint with one count of Hobbs Act robbery, in violation of Title 18 Untied States Code Section 1951, one count of narcotics possession with intent to distribute, in violation of Title 21, United States Code, Sections 812, 841(a)(1), and 841(b)(1)(B), and one count of the use of a firearm in furtherance of a crime of violence or narcotics trafficking offense, in violation of Title 18, United States Code, Sections 924(c)(1)(A)(ii). RODRIGUEZ was presented and detained by Magistrate Judge Barbara Moses. *See* Untied States v. De la Cruz Rodriguez (attached as "Exhibit B").

j. Before RODRIGUEZ was released from the hospital and was to be transferred to the custody of the Bureau of Prisons, law enforcement officers retrieved the Flip Phone from RODRIGUEZ's person.

k. A subsequent investigation revealed that DNA from trigger of the recovered firearm matched RODRIGUEZ's DNA profile maintained on a law enforcement database.

B. Probable Cause Justifying Search of the Subject Devices

9. Like individuals engaged in any other kind of activity, individuals who engage in drug distribution store records relating to their activity and to persons involved with them in that activity on electronic devices such as the Subject Devices. Such records can include, for example, logs of chats or emails with coconspirators, records of illegal transactions, contact information for other drug dealers or drug users including telephone numbers, email addresses, and identifiers for

instant messaging and social medial accounts. Individuals engaged in criminal activity often store such records in order to, among other things, (1) keep track of co-conspirator's contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, dividing those proceeds with co-conspirators; and (4) store stolen data for future exploitation.

10. Likewise, like individuals engaged in any other kind of group activity, individuals who engage in robberies use their phones to plan, coordinate, and follow-up with others involved in the activity. In my training and experience, such planning and follow-up can occur in the days and even weeks prior to and following a robbery.

11. In addition, video from the lobby of the building containing Apartment-1 depicts RODRIGUEZ using what appears to be an iPhone. Similarly, video from the apartment building where RODRIGUEZ dressed himself in the wig and dress depicts RODRIGUEZ using The iPhone's camera to look at himself. In the video, RODRIGUEZ stares at The iPhone's screen, repeatedly adjusting his wig and clothing.

12. Moreover, based on my training and experience, I also know that individuals involved in drug trafficking, use multiple phones. In particular, individuals involved in drug trafficking will maintain a cheaper phone that can be easily and often thrown out and replaced, also known as a "burner phone." Because drug traffickers do not wish to throw away expensive phones, such as The iPhone, they will buy and maintain different burner phones for short periods. The Flip Phone is the type of phone that drug traffickers will purchase as a burner phone to be used for a short period.

13. Based on the foregoing, I respectfully submit there is probable cause to believe that RODRIGUEZ is are engaged in the Subject Offenses, including drug trafficking, and that evidence of this criminal activity is likely to be found on the Subject Devices.

III. Procedures for Searching ESI

A. Review of ESI

1. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI sent, received, or obtained from the period of February 1, 2018 to May 23, 2018 on the Subject Devices for information responsive to the warrant.

2. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

3. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the Subject Device to locate all data responsive to the warrant.

B. Return of the Subject Devices

4. If the Government determines that the Subject Devices are no longer necessary to retrieve and preserve the data on the device, and that the Subject Devices are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the Subject Devices, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

IV. Conclusion and Ancillary Provisions

5. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

Tyler S. Miceli
Special Agent
Bureau of Alcohol, Tobacco, Firearms, and Explosives Special Agent

Sworn to before me on
June 7, 2018

HON. ROBERT W. LEHRBURGER
UNITED STATES MAGISTRATE JUDGE

Attachment A

I. Device Subject to Search and Seizure

The device that is the subject of this search and seizure warrant (the "Subject Devices") are described as follows:

(1) a White Model A1661 iPhone 7 Plus bearing IC 579C-E3087A; and
(2) a black LG flip phone bearing serial number 707VTEY100124 and IMEI number 359926-08-100124-3

II. Review of ESI on the Subject Device

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI sent, received, or obtained on the Subject Device for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1951 (Hobbs Act robbery); Title 21, United States Code, Sections 812, 841 (narcotics possession with intent to distribute); Title 18, United States Code, Section 924(c) (use of a firearm in furtherance of a crime of violence or narcotics trafficking offense) (the "Subject Offenses") described as follows:

1. the phone number associated with the Subject Device;

2. address books and contact lists;

3. log information of phone numbers of incoming and outgoing calls;

4. other caller-identification information, including names, phone numbers, and addresses;

5. opened and unopened voicemail messages;

6. text, data, chat, digital photographs and video, MMS (i.e., multimedia messaging service), and SMS (i.e., short message service), email messages (collectively, "text messages"), any attachments to those text messages, such as digital photographs and videos, and any associated information, such as the phone number from which the text message was sent, pertaining to the robberies, the location of the robberies, the occupants of the robbed apartments, narcotics, and narcotics trafficking,

7. calendar or other scheduling information;

8. bank records, checks, credit card bills, account information, and other financial records;

9. Evidence of user attribution showing who used or owned the Subject Device at the time the records and items described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

EXHIBIT B

AO 93 (SDNY Rev. 01/17) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

(1) a White Model A1661 iPhone 7 Plus bearing IC 579C-E3087A; and (2) a black LG flip phone bearing serial number 707VTEY100124 and IMEI number 359926-08-100124-3

Case No. 18 MAG . 4774

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of New York
(identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment A

The search and seizure are related to violation(s) of *(insert statutory citations)*:

Title 18, United States Code, Section 1951 (Hobbs Act robbery); Title 21, United States Code, Sections 812, 841 (narcotics possession with intent to distribute); Title 18, United States Code, Section 924(c) (use of a firearm in connections with a crime of violence or narcotics trafficking offense)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before _____
(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☑ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.

☐ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court. _____
USMJ Initials

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 6/4/2018

Judge's signature

City and state: New York, NY

The Honorable Robert W. Lehrburger, U.S.M.J.
Printed name and title

AO 93 (SDNY Rev. 01/17) Search and Seizure Warrant (Page 2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the Court.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Attachment A

I. Device Subject to Search and Seizure

The device that is the subject of this search and seizure warrant (the "Subject Devices") are described as follows:

(1) a White Model A1661 iPhone 7 Plus bearing IC 579C-E3087A; and
(2) a black LG flip phone bearing serial number 707VTEY100124 and IMEI number 359926-08-100124-3

II. Review of ESI on the Subject Device

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI sent, received, or obtained on the Subject Device for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1951 (Hobbs Act robbery); Title 21, United States Code, Sections 812, 841 (narcotics possession with intent to distribute); Title 18, United States Code, Section 924(c) (use of a firearm in furtherance of a crime of violence or narcotics trafficking offense) (the "Subject Offenses") described as follows:

1. the phone number associated with the Subject Device;

2. address books and contact lists;

3. log information of phone numbers of incoming and outgoing calls;

4. other caller-identification information, including names, phone numbers, and addresses;

5. opened and unopened voicemail messages;

6. text, data, chat, digital photographs and video, MMS (i.e., multimedia messaging service), and SMS (i.e., short message service), email messages (collectively, "text messages"), any attachments to those text messages, such as digital photographs and videos, and any associated information, such as the phone number from which the text message was sent, pertaining to the robberies, the location of the robberies, the occupants of the robbed apartments, narcotics, and narcotics trafficking,

7. calendar or other scheduling information;

8. bank records, checks, credit card bills, account information, and other financial records;

9. Evidence of user attribution showing who used or owned the Subject Device at the time the records and items described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.