UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against-

17-cr-0686 (LAK)

JAMES GATTO, a/k/a "Jim,"
MERL CODE, and
CHRISTIAN DAWKINS,

Defendants.

MEMORANDUM OPINION

Appearances:

Aline R. Flodr
Edward B. Diskant
Noah David Solowiejczyk
Robert Lee Boone
Eli Jacob Mark
Assistant United States Attorneys
ROBERT KHUZAMI
DEPUTY UNITED STATES ATTORNEY

Michael Steven Schachter
Casey Ellen Donnelly
WILLKIE FARR & GALLAGHER LLP

David Angeli
ANGELI LAW GROUP LLC

Attorneys for Defendant James Gatto

Andrew A. Mathias
William W. Wilkins
Mark C. Moore
NEXSEN PRUET, LLC

Johanna Rae Hudgens
WINSTON & STRAWN LLP

James Lawrence Bernard
Joel Cohen
STROOCK & STROOCK & LAVAN LLP

Attorneys for Defendant Merl Code

Jennifer L. Brown
FEDERAL DEFENDERS OF NEW YORK INC.

Steven A. Haney, Sr.
HANEY LAW GROUP PLLC

Attorneys for Defendant Christian Dawkins

LEWIS A. KAPLAN, *District Judge.*

This matter is before the Court on the joint motion of defendants Code and Dawkins to suppress evidence obtained from searches of their cell phones [DI 75].[1]

Background

Defendant Code was a consultant for "Company-1," a multi-national corporation that designs and manufactures shoes, clothing, and accessories for various sports, including basketball. Defendant Dawkins was an aspiring business manager for professional athletes. Both defendants are charged with conspiring to commit wire fraud by paying bribes to certain high school basketball

---

[1] Defendant Gatto initially joined this motion but has since withdrawn his own application. DI 144. Unless indicated otherwise, all references to docket item numbers refer to the docket in this case.

players bound for NCAA Division I universities and/or their families in exchange for commitments by the students to matriculate at specific universities and then retain Dawkins' services and sign with Company-1 upon turning professional.[2]

Defendants' Arrests

On September 25, 2017, defendants Dawkins and Code were charged in a criminal complaint with conspiracy to commit wire fraud, substantive wire fraud, and money laundering (the "Subject Offenses").[3] Dawkins was arrested on the same day and Code on the following day.[4] At the time of their arrests, each of Dawkins and Code had two cell phones on his person.[5] At the time of his arrest, Dawkins was believed by law enforcement to have been en route to a meeting with an FBI undercover agent to discuss the Subject Offenses.[6] Law enforcement personnel seized both cell

---

2 DI 39.

3 DI 1.

Dawkins was charged also in a separate case with conspiracy to commit bribery, substantive bribery, conspiracy to commit honest services fraud, substantive honest services fraud, conspiracy to commit wire fraud, and conspiracy to violate the Travel Act. No. 17-cr-684, DI 1. These charges related to alleged efforts by Dawkins to bribe certain NCAA Division I coaches in exchange for the coaches' agreement to persuade certain student-athletes in their programs to retain Dawkins' services upon leaving college and playing professional ball.

4 DI 76-3, at 2, DI 76-2 at 3.

5 DI 76-3 at 2, DI 76-2 at 2-3.

6 DI 76-3 at 6.

phones from each defendant incident to the arrests.[7]

Search Warrant Applications

On October 6, 2017[8] and November 3, 2017,[9] the government applied for warrants to search the seized cell phones. Each application stated that there was probable cause to believe that the seized cell phones contained evidence of the Subject Offenses.

The government submitted an affidavit by an FBI Special Agent ("Agent 1") in support of its application to search the two Dawkins cell phones. Agent 1 there stated that one cell phone recovered from Dawkins had been subject to an FBI wiretap and that Dawkins had been recorded using that phone for several calls and at least one text message as a part and in furtherance of the schemes with which he had been charged.[10] The agent stated also that he was aware that Dawkins had used other cell phones in connection with the Subject Offenses. As the second cell phone was recovered from Dawkins' person when he was believed to be en route to a meeting related to the alleged schemes, Agent 1 attested that he believed it likely that Dawkins had used the second cell phone to "communicate with co-conspirators in furtherance of the Subject Offenses."[11]

The government submitted an affidavit by another FBI Special Agent ("Agent 2") in

---

7 DI 76-3 at 2, DI 76-2 at 2-3.

8 DI 76-3.

9 DI 76-2.

10 DI 76-3 at 5-6.

11 *Id.* at 6.

support of its application to search the two Code cell phones. Agent 2 there stated that the first cell phone recovered from Code also had been subject to an FBI wiretap. During the period from June through September 2017, Code repeatedly was recorded using that phone to communicate regarding and in furtherance of the Subject Offenses, including several calls with defendant Dawkins to discuss the prospective payment of bribes to certain coaches.[12] Agent 2 stated that the second Code cell phone had been used by Code in a conversation with Dawkins that was intercepted over a wiretap of Dawkins' cell phone. During that conversation, Code and Dawkins discussed payments in furtherance of the Subject Offenses. On the basis of that conversation and the fact that Code was carrying this second phone with him on the day of his arrest, Agent 2 stated that he believed it likely that Code had used that phone on other occasions to communicate with his alleged co-conspirators in furtherance of the Subject Offenses.[13] He stated also that:

> "[B]ased on [his] training and experience, [he was] aware that cellphones like the Subject Devices that ha[d] been used to communicate with others about fraud schemes, often contain[ed] records of that activity, including call logs, voicemail messages, text messages, email correspondence, contact information and other identifying data regarding coconspirators, notes about calls and meetings relevant to the Subject Offenses, and the like. Indeed, individuals engaged in such criminal activity often store[d] such records in order to, among other things, keep track of coconspirators [sic] contact information and to keep a record of requests for payments along with details regarding the manner and method in which those payments were made."[14]

Both Agents 1 and 2 stated that law enforcement personnel would review the electronically stored information ("ESI") on the subject cell phones for information responsive to

---

12 DI 76-2 at 7-11.

13 *Id.* at 12.

14 *Id.* at 12-13.

the warrant. They listed several search techniques and stated that while "[l]aw enforcement personnel [would] make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant," "[d]epending on the circumstances, . . . law enforcement [might] need to conduct a complete review of all the ESI from the Subject Devices to locate all data responsive to the warrant."[15]

Search Warrants Issued

The government's applications were granted and search warrants were issued in respect of the Dawkins and Code cell phones on October 6, 2017[16] and November 3, 2017,[17] respectively. Each warrant authorized law enforcement personnel to "review the ESI contained on the Subject Devices for evidence, fruits, and instrumentalities" of the charged schemes – namely, (1) in the case of Dawkins, evidence of schemes to "(i) pay NCAA coaches in exchange for those coaches using their influence with NCAA players to convince those players and/or their families to retain certain agents, financial advisors, and others; and (ii) pay high school and NCAA players and conceal those payments from universities, thereby defrauding those universities of scholarship money and of the right to control their assets"[18] and, (2) in the case of Code, evidence of "schemes to make payments from the universities attended or intended to be attended by the players, thereby

---

15 DI 76-3 at 7, DI 76-2 at 14.

16 DI 76-6.

17 DI 76-5.

18 DI 76-6 at 3.

defrauding those universities of scholarship money and of the right to control their assets."[19] In each case, the warrant specified the categories of evidence responsive to the warrant.[20]

Both warrants tracked the language in the applications with respect to the procedures for finding such evidence. Each listed various targeted search techniques, but stated also that "[d]epending on the circumstances, a complete review of the seized ESI may require examination of all of the seized data to evaluate its contents and determine whether the data is responsive to the warrant."[21]

Motion to Suppress

Defendants Dawkins and Code filed this motion to suppress evidence derived from the searches of their cell phones. They argued that the warrants (1) did not establish probable cause to seize and search defendants' cell phones and, in the alternative, (2) were facially overbroad because they did not limit the scope of the searches to the locations of data for which there was

---

19 DI 76-5 at 3.

20 DI 76-6 at 3-4 (providing that such "evidence, fruits, and instrumentalities" included, for example, "evidence, including communications regarding, criminal conduct involving financial transactions, favors or benefits to NCAA coaches or other NCAA advisors in order to influence student-athletes at universities, in violation of those officials' duties of honest services to their employers, the laws prohibiting wire fraud, and the laws prohibiting bribery[,] . . . actions taken by NCAA coaches or other NCAA advisors relating to student-athletes for the benefit of individuals providing benefits to such coaches and advisors, in violation of those coaches or advisors' duties of honest services to their employers, the laws prohibiting wire fraud, and the laws prohibiting bribery[,] payments to high school or college athletes[, and] of the identity of individuals receiving benefits or official action in return for financial transactions, favors, or other benefits provided, facilitated, or discussed by the users of the Subject Device"); DI 76-5 at 3-4 (same).

21 DI 76-6 at 4; DI 76-5 at 4.

probable cause to search. Accordingly, defendants argued, any law enforcement officers' reliance on the search warrants was unreasonable. The government opposed the motion, and the Court heard oral argument on March 22, 2018.

At oral argument, the Court invited the government to submit an affidavit focused on how data on a smart phone is stored and "the difficulties in separating out the data" into various categories, such as images, contacts, call logs, etc.[22] The government subsequently submitted the affidavit of another FBI Special Agent ("Agent 3").[23]

Agent 3 stated that although the search warrants had permitted a broad review of the ESI from the seized cell phones, no such "complete review" of all of the seized data actually occurred.[24] For each of the cell phones (except a Blackberry recovered from defendant Code), the law enforcement agents reviewing the data extracted a copy of the contents of the phones using a program called "Cellebrite." The Cellebrite program automatically divided the content of each of the cell phones by category of data, such as "SMS Messages, "Emails, "Voicemails," etc., and then facilitated law enforcement agents' search of the relevant categories of data by providing a "user-friendly interface to search a Cellebrite Extraction of a phone using common search terms and methodologies."[25] With respect to these cell phones, Agent 3 stated that he and "other law enforcement agents focused on data categories such as MMS Messages, SMS Messages, Chats,

---

22 DI 130 at 24:23-25:3, 28:1-5.

23 DI 132-1.

24 *Id.* at 5, 7.

25 *Id.* at 4.

Contacts, Call Logs, and Voice Messages, all of which [they] believed were most likely to contain communications or related information regarding or in furtherance of the criminal scheme charged."[26] In those data categories, the agents generally conducted their review using search terms, but on occasion executed individual review without using search terms. For the remaining categories of data, such as "Device Location," "Device Notifications," "Web History," and "Images," the agents conducted only "a cursory review sufficient to satisfy [them]selves that nothing in that category of data was likely to constitute Identified Material."[27] With respect to "Images" specifically, Agent 3 stated that if the Images category consisted primarily of photographs, he did not review particular photographs. But if the images "contained documents or spreadsheets, [he] did review at least some of those items to determine whether they were within the scope of the Search Warrants."[28]

Defendant Code's Blackberry, on the other hand, was not compatible with the Cellebrite program and thus had to be reviewed manually.[29] Agent 3 personally conducted that review and focused on the text messages contained on the phone, the contacts, and certain documents and/or spreadsheets saved on the phone. Aside from those categories of data, he reviewed no other area of the Blackberry.[30]

---

26 *Id.* at 5.

27 *Id.* at 6.

28 *Id.*

29 *Id.* at 7.

30 *Id.*

Discussion

Probable Cause

Defendants first argue that probable cause to search the entirety of defendants' cell phones did not follow from the mere fact that defendants used those cell phones to make calls and send text messages related to the charges brought against them.[31] In response, the government argues that it follows from the fact that defendants used their phones to make calls that "the phones would . . . include 'call logs' reflecting the fact of the calls; saved 'contacts' including the names and phone numbers of the co-conspirators with whom the defendant spoke on each occasion; and other communications between that defendant and those co-conspirators, including voice messages, text messages, and e-mails, relevant to the same subjects, *i.e.*, the charged schemes."[32]

The requirement that law enforcement personnel obtain a search warrant before searching a cell phone seized incident to arrest was articulated by the Supreme Court in *Riley v. California*.[33] The Court there found a substantial privacy interest in the data contained in a cell phone.[34] However, a search warrant need be supported only by probable cause, not a *prima facie*

---

31 DI 76 at 8-10 ("Permitting a search of all of the data stored on Defendants' cell phones based on the fact that they used them to make phone calls is no different than permitting the Government to search the photo albums and videotapes found in a person's home simply because that person made phone calls from his landline.").

32 DI 117 at 38.

33 134 S. Ct. 2473 (2014).

34 *Id.* at 2488-91 (2014); *see id.* at 2489 ("[M]any [cell phones] are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

showing of criminal activity.[35] And defendants here would require a showing that would go beyond establishing probable cause.

Whether there is probable cause to support the issuance of a search warrant depends on the "totality of the circumstances."[36] "The issuing judicial officer must 'make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.'"[37] The probable cause standard "does not demand any showing that a good-faith belief be 'correct or more likely true than false.'"[38] Rather, "[i]t requires only such facts as make wrongdoing or the discovery of evidence thereof probable."[39] Thus, a sufficient nexus between the alleged criminal activities and the place to be searched "does not require direct evidence and may be based on reasonable inference from the facts presented based on common sense and experience."[40]

---

35 *United States v. Wagner*, 989 F.2d 69, 72 (2d Cir. 1993).

36 *Id.* at 71-72.

37 *Id.* at 72 (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)); *accord Walczyk v. Rio*, 496 F.3d 139, 156 (2d Cir. 2007).

38 *Walczyk*, 496 F.3d at 157 (quoting *Texas v. Brown*, 460 U.S. 730, 742 (1983)).

39 *Id.*

40 *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004) (internal quotation marks and citations omitted); *see also Walczyk*, 496 F.3d at 156 ("In assessing probabilities, a judicial officer must look to the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." (internal quotation marks omitted) (quoting *Illinois*, 462 U.S. at 231)).

Moreover, "[a] reviewing court must accord substantial deference to the finding of an issuing judicial officer that probable cause exists."[41] This Court's determination thus is limited "to whether the issuing judicial officer had a substantial basis for the finding of probable cause."[42] A court need not suppress evidence obtained pursuant to a search warrant, "even if the affidavits submitted in support of the search warrant did not evince probable cause," unless the "'affidavit [is] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.'"[43]

The Court concludes, in the case of each of the warrants at issue, that the magistrate judge was entitled to infer from the fact that the defendant used a cell phone to make calls and send text messages related to the alleged scheme that other communications and evidence pertaining to that scheme also would have been made on that cell phone.[44] This conclusion reasonably reaches

---

41 *Wagner*, 989 F.2d at 72 (citations omitted).

42 *Singh*, 390 F.3d at 181 (internal quotation marks omitted) (quoting *Wagner*, 989 F.2d at 72).

43 *Id.* (quoting *United States v. Leon*, 468 U.S. 897, 923 (1984)).

44 Indeed, in his affidavit supporting the application to search defendant Code's cell phones, Agent 2 stated also that, "based on [his] training and experience, [he was] aware that cellphones like the Subject Devices that ha[d] been used to communicate with others about fraud schemes, often contain[ed] records of that activity, including call logs, voicemail messages, text messages, email correspondence, contact information and other identifying data regarding coconspirators, notes about calls and meetings relevant to the Subject Offenses, and the like." DI 76-2 at 12-13; *cf. Singh*, 390 F.3d at 181-83 (affirming validity of warrant to search defendant's residence after defendant's co-worker provided information about the role that the defendant's wife played in maintaining billing and accounts payable records at their residence and FBI agent stated that "in her nine years of experience in working on health care fraud and drug-distribution cases, she found that . . . people frequently maintained financial and bank records at their homes or businesses and kept such records for a number of years").

The case is closer with respect to the second cell phone recovered from defendant Dawkins

not just other forms of communication, but other forms of data that may be related to or embedded in such communications – in other words, contacts and call logs as well as documents or images that may have been embedded in or otherwise related to a communication made using the cell phone.

A judge's probable cause determination is made on the basis of "common sense and experience."[45] Given the substance of the supporting affidavits and the magistrate judges' respective conclusions that probable cause existed, it was far from "entirely unreasonable" for the government to have assumed that there was probable cause to believe that the seized cell phones contained evidence of the alleged schemes.

Alleged Overbreadth

Code and Dawkins next argue that evidence obtained from their cell phones must be suppressed because the search warrants were overbroad in permitting the government, "[d]epending on the circumstances, . . . [to] examin[e] . . . all of the seized data to evaluate its contents and determine whether the data is responsive to the warrant."[46] Defendants argue that "[t]o the extent that this Court concludes that the Warrants established probable cause to seize and search

---

incident to his arrest. This cell phone was not wiretapped or otherwise recorded. Accordingly, law enforcement had no information confirming whether the cell phone had been used for communications related to the Subject Offenses. However, the statement by Agent 1 that Dawkins' was believed to have been on his way to a meeting related to the alleged schemes, combined with the belief that Dawkins' had used numerous cell phones to conduct the alleged schemes, provided a sufficiently substantial basis for the magistrate judge to have concluded that probable cause existed.

45 *Singh*, 390 F.3d at 182.

46 DI 76-6 at 4, DI 76-5 at 4; *see also* DI 76 (Def. Br.) at 10-11 ("The Warrants in no way limited the scope of the authorized search to the locations of electronic data on the phone for which there would be probable cause to believe evidence of a crime may be found.").

Defendants' phones in any manner, the search of those phones should have been limited to the locations on the phones where, according to the Applications, there was probable cause to conclude evidence of criminality would be found."[47]

Defendants' argument pertains to the Fourth Amendment's prohibition of "'wide-ranging exploratory searches' unsupported by probable cause."[48] The Fourth Amendment mandates "that a search warrant describe with particularity the place to be searched and the persons or things to be seized."[49] To be sufficiently particularized, a warrant must, (1) "identify the specific offense for which the police have established probable cause," (2) "describe the place to be searched," and (3) "specify the items to be seized by their relation to designated crimes."[50]

In *United States v. Rosa*,[51] for example, the Second Circuit held that a warrant to search a defendant's electronic devices for evidence of child pornography was defective because the warrant stated only that the county sheriff's office was authorized to search the defendant's entire residence for any electronic equipment or digital information "which would tend to identify criminal conduct."[52] It was clear from the application for the warrant and its supporting documents that the

---

47 *Id.* at 13-14.

48 *United States v. Rosa*, 626 F.3d 56, 61 (2d Cir. 2010) (quoting *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)).

49 *Id.*

50 *United States v. Ulbricht*, 858 F.3d 71, 99 (2d Cir. 2017) (internal quotation marks omitted) (quoting *United States v. Galpin*, 720 F.3d 436, 445-46 (2d Cir. 2013)).

51 *Rosa*, 626 F.3d 56.

52 *Id.* at 58 (quoting search warrant).

search in fact had been intended to target specific types of evidence as they related to specific offenses – namely, "any and all electronic equipment potentially used in connection with the production or storage of child pornography and any and all digital files and images relating to child pornography contained therein."[53] The warrant therefore was overbroad because it "failed to describe with particularity the evidence sought and, more specifically, to link that evidence to the criminal activity supported by probable cause."[54]

But here, the warrants readily met all three particularity requirements. The warrants each listed the criminal offenses with which defendants had been charged in the relevant criminal complaints. Each warrant described also the places – *i.e.*, the specific cell phones – to be searched. And each specified exactly the types of content that fell within the scope of the warrant.[55]

Nor were the warrants rendered invalid by virtue of their having authorized searches of the entirety of the cell phones for data responsive to the warrants. In *United States v. Ulbricht*,[56] the Second Circuit concluded that a warrant authorizing the search of an entire laptop for specific types of evidence related to an alleged criminal enterprise was not overly broad. There, the Circuit stated:

> "A warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material, without violating

---

53 *Id.* at 62.

54 *Id.*

55 DI 76-6 at 3-4 (delineating relevant criminal statutes, describing target cell phones, and listing types of responsive evidence), DI 76-5 at 3-4 (same).

56 *Ulbricht*, 858 F.3d 71.

> the particularity requirement. For example, a warrant may allow the government to search a suspected drug dealer's entire home where there is probable cause to believe that evidence relevant to that activity may be found anywhere in the residence. Similarly, "[w]hen the criminal activity pervades [an] entire business, seizure of all records of the business is appropriate, and broad language used in warrants will not offend the particularity requirements." *U.S. Postal Serv. v. C.E.C. Servs.*, 869 F.2d 184, 187 (2d Cir. 1989). Ulbricht used his laptop to commit the charged offenses by creating and continuing to operate Silk Road. Thus, a broad warrant allowing the government to search his laptop for potentially extensive evidence of those crimes does not offend the Fourth Amendment, as long as that warrant meets the three particularity criteria . . . ."[57]

As was the case in *Ulbricht*, law enforcement personnel here came across personal data that was unrelated to defendants' alleged crimes.[58] "Such an invasion of a criminal defendant's privacy is inevitable, however, in almost any warranted search because in 'searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.'"[59]

Here, in particular, it would have been difficult for the search warrants to specify *ex ante* those areas of data in which law enforcement was likely to find evidence responsive to the warrants because, among other reasons, it was not clear in advance whether the government would be able to sort through the various data categories in some automatic or mechanical way.[60] Indeed,

---

57 *Id.* at 102-03.

58 Agent 3 stated in his affidavit that he had cursorily reviewed certain types of data "sufficient to satisfy [him]self that nothing in that category of data was likely to constitute [evidence responsive to the warrant]." DI 132-1 at 6.

59 *Ulbricht*, 858 F.3d at 103 (quoting *United States v. Ganias*, 824 F.3d 199, 211 (2d Cir. 2016)).

60 *Ganias*, 824 F.3d at 213 ("[I]n assessing the reasonableness, for Fourth Amendment purposes, of the search and seizure of digital evidence, we must be attuned to the technological features unique to digital media as a whole and to those relevant in a particular

not all of the phones were compatible with the Cellebrite program. And in the cases of those that were so compatible, the data categories were not perfectly separable. For example, certain messages were able to "include or 'attach' various forms of multimedia, such as images and videos."[61] Moreover, the Cellebrite program combined photographs and documents in the broad category of "Images."[62]

Because the Court finds that the three requirements of particularity were met in the case of both search warrants, it finds that neither warrant was overbroad in violation of the Fourth Amendment.

Good Faith Exception

Suppression would not be warranted even if this Court were to find that probable cause was lacking or that either search warrant was overbroad. Evidence obtained in violation of the Fourth Amendment is excluded only as a "last resort."[63] As the Second Circuit has stated:

> "Application of the exclusionary rule depends on the 'efficacy of the rule in deterring Fourth Amendment violations in the future' as well as a determination that 'the benefits of deterrence . . . outweigh the costs.' [*Herring v. United States*, 555 U.S. 135, 141 (2009)]; *see also United States v. Julius*, 610 F.3d 60, 66 - 67 (2d Cir. 2010) (discussing *Herring*). Moreover, '[t]he extent to which the exclusionary rule is justified by these deterrence principles varies with the culpability of the law

---

case–features that simply do not exist in the context of paper files."); *see also id.* 212-15 (distinguishing generally between a digital hard drive and a physical file cabinet).

61 DI 132-1 at 4 n.1.

62 *Id.* at 6.

63 *Rosa*, 626 F.3d at 64 (internal quotation marks omitted) (quoting *Herring v. United States*, 555 U.S. 135, 140 (2009)).

> enforcement conduct.' *Herring*, [555 U.S. at 143]. Thus, in deciding to suppress evidence, we look to whether 'police conduct [is] sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.' *Id.*; *see also United States v. Leon*, 468 U.S. 897, 911, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984) ("[A]n assessment of the flagrancy of the police misconduct constitutes an important step in the calculus."). 'The pertinent analysis of deterrence and culpability is objective,' and '"our good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal" in light of "all of the circumstances."' *Herring*, [555 U.S. at 145] (quoting *Leon*, 468 U.S. at 922 n. 23, 104 S. Ct. 3405)."[64]

In this case, as in *Rosa*, defendants set forth no evidence that law enforcement behaved in a deliberately unlawful manner or lacked a good faith belief in the validity of the search warrants. Accordingly, there would be no meaningful deterrence in suppressing the evidence obtained from the searches of Code's and Dawkins' cell phones. Suppression therefore would be unwarranted.[65]

---

64 *Id.*

65 *Id.* at 64-66.

Conclusion

For the foregoing reasons, defendants' joint motion to suppress evidence obtained from searches of their cell phones [DI 75] is denied.

SO ORDERED.

Dated: June 1, 2018

Lewis A. Kaplan.
United States District Judge