24-0824-cr

United States Court of Appeals

for the

Second Circuit

UNITED STATES OF AMERICA,

Appellee,

– v. –

EZHIL KAMALDOSS, AKA Kamaldoss Sezhian,
AKA Kamal Doss, AKA Ezhil Cezhian,

Defendant-Appellant,

VELAUDAPILLAI NAVARATNARAJAH, AKA Rajah,

Defendant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

REPLY BRIEF FOR DEFENDANT-APPELLANT

BRIAN E. SPEARS
LESLIE A. CAHILL
SPEARS MANNING & MARTINI LLC
Attorneys for Defendant-Appellant
2425 Post Road, Suite 203
Southport, Connecticut 06890
(203) 292-9766

CP COUNSEL PRESS (800) 4-APPEAL • (378274)

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES ii

INTRODUCTION 1

I. The District Court Erred in Denying Mr. Kamaldoss's Motion to Suppress 1

A. Mr. Kamaldoss Was in Custody When He Surrendered the Passwords to his Electronic Devices 1

B. A Warrant Was Required to Conduct Forensic Searches of Mr. Kamaldoss's Electronic Devices 8

C. Even if a Warrant Was Not Required, the Search Should Have Been Limited to Detecting Contraband 13

D. This Court Should Decline to Apply the Good Faith Exception 17

E. Any Error Was Not Harmless 19

II. The Two-Level Sentencing Enhancement for "Mass Marketing by Means of an Interactive Computer Service" Was Imposed Without a Sufficient Factual Basis or Explanation 22

CONCLUSION 23

TABLE OF AUTHORITIES

Page(s)

Cases:

Davis v. United States,
564 U.S. 229 (2011) 18

Hoffman v. United States,
341 U.S. 479 (1951) 6

Riley v. California,
573 U.S. 373 (2014) 8, 10, 16

Rossi v. Town of Pelham,
35 F. Supp. 2d 58 (D.N.H. 1997) 3

United States v. Cano,
934 F.3d 1002 (9th Cir. 2019) 15

United States v. Djibo,
151 F. Supp. 3d 297 (E.D.N.Y. 2015) 5, 7

United States v. FNU LNU,
653 F.3d 144 (2d Cir. 2011) 5

United States v. Fox,
No. 23-CR-227 (NGG), 2024 WL 3520767 (E.D.N.Y. July 24, 2024) 11

United States v. Ganias,
824 F.3d 199 (2d Cir. 2016) 18

United States v. Greenfield,
831 F.3d 106 (2d Cir. 2016) 7

United States v. Johnson,
457 U.S. 537 (1982) 18

United States v. Levy,
803 F.3d 120 (2d Cir. 2015) 13, 14

United States v. Molina-Gomez,
781 F.3d 13 (1st Cir. 2015).....5, 15

United States v. Patane,
542 U.S. 630 (2004).....7

United States v. Place,
462 U.S. 696 (1983).....3

United States v. Shvartsman,
722 F. Supp. 3d 276 (S.D.N.Y. 2024).....5, 6

United States v. Smith,
673 F. Supp. 3d 381 (S.D.N.Y. 2023), *appeal docketed*
(2d Cir. June 25, 2024)..... 8, 9, 10

United States v. Smith,
967 F.3d 198 (2d Cir. 2020)..... 11, 12, 14, 16

United States v. Stewart,
907 F.3d 677 (2d Cir. 2018).....6

United States v. Sultanov,
742 F. Supp. 3d 258 (E.D.N.Y. July 24, 2024)..... 10, 11

United States v. Taylor,
745 F.3d 15 (2d Cir. 2014).....20

United States v. Touset,
890 F.3d 1227 (11th Cir. 2018).....9

Statutes & Other Authorities:

47 U.S.C. § 230(f)(2).....23

U.S.S.G. § 2D1.1 22

INTRODUCTION

Defendant-Appellant Ezhil Kamaldoss ("Mr. Kamaldoss") respectfully submits this Reply Brief in response to the Brief filed by the Appellee, the United States ("Govt. Br.") and advances the following points in support thereof.

I. The District Court Erred in Denying Mr. Kamaldoss's Motion to Suppress.

A. *Mr. Kamaldoss Was in Custody When He Surrendered the Passwords to his Electronic Devices*

As Mr. Kamaldoss explained in his opening brief, following his arrival, with his family, at John F. Kennedy International Airport ("JFK") on April 23, 2019, he was referred to secondary inspection by Customers and Border Protection ("CBP") in response to a "lookout" that had been entered for Mr. Kamaldoss in the CBP system. Without issuing *Miranda* warnings, CBP officers solicited and obtained from Mr. Kamaldoss the passwords to his laptop and cell phone, which were forensically imaged by an agent with the Department of Homeland Security, Homeland Security Investigations while Mr. Kamaldoss and his family were questioned in a smaller private room

before his devices were returned to him nearly two and a half hours later. Mr. Kamaldoss understood, correctly, that he was not free to leave throughout this encounter, during which he was questioned in a manner designed to gather information about an ongoing criminal investigation in which Mr. Kamaldoss was a target.

Despite these circumstances, the government repeatedly dismisses Mr. Kamaldoss's experience in secondary inspection as tantamount to being at the DMV. Govt. Br. at 16, 25, 30. While it is true that Special Agent Chunton compared the secondary inspection waiting area to the DMV, A-379, the overarching analogy is inapt given the evidence that the first room to which Mr. Kamaldoss was referred contained ten or more armed and uniformed law enforcement officers and chairs with handcuffs attached to them, *see* A-404-05, and that Mr. Kamaldoss's liberty was unequivocally restricted. The government claims that Mr. Kamaldoss was not "free to leave" only in the sense that he had not yet been admitted to the United States, and thus he could have returned to India had his admission been denied. Govt. Br. at 28-29. However, nowhere does the record indicate that Mr. Kamaldoss was

informed that he would be free to leave on a flight to India if he did not clear secondary inspection. Moreover, a reasonable person in his position would not have concluded that he would be at liberty to return to his home country if he did not pass CBP inspection, especially given that he had surrendered his luggage, wallet, phone and laptop at various points during the interrogation. *Cf. Rossi v. Town of Pelham*, 35 F. Supp. 2d 58, 72 (D.N.H. 1997) ("By seizing the traveler's luggage, the government agents had put the traveler to the choice between his interests in liberty and property, because if he chose to leave the airport, he would be abandoning his luggage to the seizing agents. Traveling without luggage and its contents would be impracticable, so the traveler's freedom to leave was empty, and his decision to remain with his luggage was not entirely a product of voluntary choice but was, to one degree or another, coerced") (citing *United States v. Place*, 462 U.S. 696, 709 (1983)). Indeed, as Special Agent Chunton confirmed, Mr. Kamaldoss was not free to "walk out the door" "because we still ha[d] his documents." A-414.

Even more problematically, the government's brief minimizes the significance of what the District Court described as "the strongest evidence weighing in favor of a finding that Mr. Kamaldoss was in custody," *i.e.*, "the fact that he was asked for the passcodes to his electronic devices." SPA-17. In rejecting this fact as insufficient to establish a custodial interrogation, the government overlooks the context in which the request was made – to further a criminal investigation into Mr. Kamaldoss. *See* A-388 (testimony of Special Agent Chunton confirming that the purpose of the border stop was to further the criminal investigation); A-398 (testimony that a "full dump" or "imaging" of a phone is protocol when an individual is "a target of our investigation").

The government is correct that the subjective view of the questioner is not a factor in determining whether an individual is in *Miranda* custody. But the fact that Mr. Kamaldoss was exposed to a specific type of questioning--*i.e.*, that designed to elicit vast quantities of highly personal and potentially incriminating information stored on his cell phone and laptop—*is* relevant to determining whether the questioning was routine and confined to the

issue of Mr. Kamaldoss's entry into the country. *See United States v. Molina-Gomez*, 781 F.3d 13, 23 (1st Cir. 2015) (concluding that "probing questions about potential illegal activity" contributed to determination that defendant was in custody, as they "went above and beyond a routine Customs inspection"); *United States v. Djibo*, 151 F. Supp. 3d 297, 306 (E.D.N.Y. 2015) ("[P]ractically speaking, the *most* important factor in determining whether *Miranda* applies at our borders will often be the objective function of the questioning") (quoting *United States v. FNU LNU*, 653 F.3d 144, 156 (2d Cir. 2011) (Jacobs, *J.*, concurring)). That Special Agent Chunton indicated that he had arranged a border stop to image a target's electronic devices only "more than a dozen" times in his career, A-398, underscores that the type of questioning to which Mr. Kamaldoss was subjected was far from routine. *See United States v. Shvartsman*, 722 F. Supp. 3d 276, 326 (S.D.N.Y. 2024) (noting that "when Officer Gonzalez asked Garelick for his cellphone and passcode, Officer Gonzalez strayed from the routine questioning a reasonable traveler would expect at the border," but ultimately concluding defendant was not in custody when "the overall focus of Officer Gonzalez's

questioning during the secondary inspection remained on matters relevant to admissibility").

The government also argues that even if Mr. Kamaldoss was in custody, the only remedy would be suppression of the passwords themselves, which are not inherently incriminating, and not suppression of the derivative evidence that was accessed through the passwords to the electronic devices. Govt. Br. at 31-34. The Fifth Amendment privilege, however, extends not only "to answers that would in themselves support a conviction under a criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a crime." *United States v. Stewart*, 907 F.3d 677, 684 (2d Cir. 2018) (quoting *Hoffman v. United States*, 341 U.S. 479, 486 (1951)) (internal ellipses omitted); *see also Shvartsman*, 722 F. Supp. 3d at 316–20 (explaining that "[a]lthough the passcode was not '*directly* or *inherently* self-incriminating,' the Fifth Amendment applies with equal force to testimonial statements that 'may lead to incriminating evidence,'" and holding that the "foregone

conclusion" doctrine does not extend to a passcode) (quoting *United States v. Greenfield*, 831 F.3d 106, 127 (2d Cir. 2016)).

The crux of the government's argument on this point appears to be that the fruit of the poisonous tree rule does not apply to the electronic evidence obtained derivatively from Mr. Kamaldoss's statement providing his passwords. Govt. Br. at 33 (citing, *inter alia*, *United States v. Patane*, 542 U.S. 630 (2004)). However, the line of doctrine the government cites cannot be squared with the fundamentally different nature of electronic devices and the access that they provide to the totality of an individual's private life. *See Djibo*, 151 F. Supp. 3d at 310 (ordering suppression of documents obtained as a result of the defendant providing the passcode to this phone at the border and declining to apply *Patane* for a variety of reasons, including because of the manner in which a cell phone passcode provides "the proverbial 'key to a man's kingdom'"). Contrary to the government's assertion, there are sound reasons to apply the exclusionary rule in this circumstance, given the far-reaching consequences of the unlawful interrogation.

Even if the contents of the cell phone and laptop evidence would not be subject to suppression on the basis of a *Miranda* violation, however, this does not alter the fact that a warrant was required to search these devices, as discussed further below. *See United States v. Smith*, 673 F. Supp. 3d 381, 388 n.3, 394 (S.D.N.Y. 2023) (finding that *Miranda* would not require exclusion of the physical evidence obtained after defendant provided the passcode to this phone, but separately holding that a warrant was required to copy and search the phone at the border), *appeal docketed* (2d Cir. June 25, 2024).

B. *A Warrant Was Required to Conduct Forensic Searches of Mr. Kamaldoss's Electronic Devices*

In responding to Mr. Kamaldoss's Fourth Amendment argument, the government does not even acknowledge the recent cases from within this Circuit that have held that, under *Riley v. California*, 573 U.S. 373 (2014), a warrant is required to conduct a forensic search of a cell phone at the border. Appellant's Br. at 28-29. The government instead cites cases from the First, Eleventh, and Seventh Circuits for the prospect that *Riley* does not limit the border search exception in the context of electronic devices. Govt. Br. at 40-41. As these cases establish, the need to protect the border is the *sine qua non*

of the Fourth Amendment inquiry under the border search exception. *See, e.g.*, *United States v. Touset*, 890 F.3d 1227, 1234 (11th Cir. 2018) ("Although it may intrude on the privacy of the owner, a forensic search of an electronic device is a search of property. And our precedents do not require suspicion for intrusive searches of any property at the border."). This unilateral reasoning, however, ignores the critical distinction between the government's interest in searching the contents of electronic devices and its interest in searching other forms of property when it comes to safeguarding the border.

As Mr. Kamaldoss explained in his opening brief, the border search exception was born of the need to enable customs officials to locate items being smuggled into the United States, not to allow for searches of evidence that exists far beyond the border. Appellant's Br. at 30-31. Recent decisions within this Circuit have recognized this very point. Yet the government has failed to address this caselaw. *See Smith*, 673 F. Supp. 3d at 395 ("[W]hile the Court acknowledges the Government's strong interest in searching persons or physical objects at the border, any corresponding interest in searching the

digital data 'contained' on a particular physical device located at the border is relatively weak."); *United States v. Sultanov*, 742 F. Supp.3d 258, 286 (E.D.N.Y. July 24, 2024) (noting that "searching cell phone data does little to promote the specific governmental interests that the border search exception was designed to protect").

Additionally, the government's interest in border protection must be balanced against the immense privacy interests that inhere in the contents of a cell phone or laptop. In *Riley*, the "heightened government interests at stake" on which the search incident to arrest exception is based could not overcome those privacy interests in the context of what are often "volatile arrest situation[s]." *Riley*, 573 U.S. at 391. Those cases that *have* confronted the enormity of the privacy interests at stake in this context have reached only one conclusion: that a warrant is required to undertake such an invasive and far-reaching search. *See Smith*, 673 F. Supp. 3d at 395 ("Technological and cultural changes now mean that nearly all travelers carry with them, in additional to any physical items, a digital record of more information than could likely be found through a thorough search of that person's home, car,

office, mail, and phone, financial and medical records, and more besides. No traveler would reasonably expect to forfeit privacy interests in all this simply by carrying a cell phone when returning home from an international trip."); *Sultanov*, 742 F.Supp.3d at 286 ("Until technology that can translate people's brain activity . . . meaningfully advances, reviewing the information in a person's cell phone is the best approximation government officials have for mindreading") (quotation marks and footnote omitted); *United States v. Fox*, No. 23-CR-227 (NGG), 2024 WL 3520767, at *10 (E.D.N.Y. July 24, 2024) ("[O]ne does not forfeit his or her privacy rights in a device that keeps a digital record of nearly every aspect of one's life whenever they cross the border after a vacation or business trip").

The subsequent warrantless searches of Mr. Kamaldoss's devices, which were undertaken by Special Agent Connor on May 2 and May 11, 2019, further underscore the monumentally greater privacy interests that are implicated by the border search of an electronic device versus a border search of other types of property. *See United States v. Smith*, 967 F.3d 198, 207, 210 (2d Cir. 2020) (highlighting "the special concerns that apply when

law enforcement seize and search people's personal electronic data and communication devices," noting that "the Fourth Amendment imposes a time-sensitive duty to diligently apply for a search warrant if an item has been seized for that very purpose, and all the more so if the item has been warrantlessly seized," and holding that month-long delay in seeking warrant for defendant's tablet computer was unreasonable under the Fourth Amendment).

The government argues, without citing any authority, that law enforcement's subsequent forensic review of copies of data obtained at the border "is a continuation of the search initiated at the moment of detention" and is thus an extension of the border search itself, apparently regardless of the length of time that passes between the initial search and subsequent review. Govt. Br. at 44. The government does not attempt to defend the unmoored "proximity and relatedness" standard articulated by the District Court to justify such a subsequent search, which Mr. Kamaldoss challenged in his opening brief. Appellant's Br. at 32–35. Given the concerns this Court articulated in *Smith*, 967 F.3d 198, regarding the delay in seeking a warrant

for electronic data, it was error for the District Court to hold, effectively, that the May 2019 searches related back to the border search and were therefore not unreasonable.

For these reasons and those set forth in Mr. Kamaldoss's opening brief, this Court should follow *Riley* and conclude that a warrant is required to conduct a search as invasive as that involving the forensic imaging of a cell phone or laptop – at the border or otherwise.

C. *Even if a Warrant Was Not Required, the Search Should Have Been Limited to Detecting Contraband*

In arguing that the border search exception is not limited to a search for contraband, the government relies principally on this Court's decision in *United States v. Levy*, 803 F.3d 120, 123 (2d Cir. 2015), which held that reasonable suspicion for a boarder search may derive from another federal agency's investigation and not only from what the CBP official observes of the traveler him or herself. *Levy*, however, involved CBP's authority to examine and photocopy a notebook containing the defendant's handwritten notes. The defendant was the target of a criminal investigation and had returned from a business trip to Miami International Airport with the

expectation of facing criminal charges. *See id.* at 121. This Court held that that because the search of Levy's notebook was supported by reasonable suspicion that Levy was engaged in financial crimes, the border search was lawful. *See id.* at 123–24.

This Court in *Levy* did not address the question presented here—the applicability of the border exception to a traveler's cell phone or laptop. The search of a notebook bears no resemblance to the search of an individual's electronic devices. This Court has more recently observed that "the search and seizure of personal electronic devices like a modern cell phone or tablet computer implicates different privacy and possessory concerns than the search and seizure of a person's ordinary personal effects." *Smith*, 967 F.3d at 208. The Court has accordingly instructed that the "significance of this distinction [is] vital to assessing the importance of the seized property to a defendant when the item in question is a tablet computer or other personal electronic device." *Id.* As the District Court noted in Mr. Kamaldoss's case, this Court "has not spoken to the scope of a forensic search at the border,"

SPA-24, and given the caselaw that has evolved post-*Riley*, there is good reason to depart from the approach advocated by the government.

The government also argues that applying the standard adopted by the Ninth Circuit in *Cano* would result in limiting border searches of electronic devices to searches for child pornography. Govt. Br. at 43 (citing *United States v. Cano*, 934 F.3d 1002 (9th Cir. 2019)). However, electronic devices may also be used to conceal or smuggle non-digital contraband, and nothing in the *Cano* standard should limit the government's ability to search such devices manually based upon reasonable suspicion that the device was being used for this purpose. *See, e.g.*, *Molina-Gomez*, 781 F.3d at 17, 20 (discussing heroin packets that defendant had hidden inside compartments of his laptop and Playstation, and upholding border search based on reasonable suspicion that defendant was attempting to smuggle narcotics).[1]

[1] While the Ninth Circuit held that a border search is limited to the search for digital contraband, it acknowledged that there was no dispute "that a border official could, consistent with the Fourth Amendment, examine the physical body of a cell phone to see if the phone itself is contraband . . . or if the phone itself presents a physical threat to officers." 934 F.3d at 1014 n.5.

Nor would it limit the government's ability to search a traveler's other personal effects—whether "a cigarette pack, a wallet, or a purse," *Smith*, 967 F.3d at 208 (quoting *Riley*, 573 U.S. at 393), or a notebook, as was the case in *Levy*.

The bottom line is that there is nothing in this Court's precedents that specifically authorizes a search as intrusive and far-reaching as the search of an electronic device at the border based upon reasonable suspicion that the device may contain evidence of a crime. The concern in this case is greater still, where reasonable suspicion derives not from CBP's direct observations or questioning of the traveler at the border, but from a separate preexisting law enforcement investigation. Applying *Levy* to these facts without countenancing this distinction would contravene *Riley's* mandate that the traveler's immense privacy interests be balanced against the government's interest in conducting the search. Mr. Kamaldoss respectfully submits that if this Court determines that a warrant is not required, the Court should still undertake the inquiry that *Riley* requires in the first instance to hold that

reasonable suspicion of the presence of contraband is required to authorize a search of a phone or laptop at the border.

D. *This Court Should Decline to Apply the Good Faith Exception*

The government argues that the good faith exception applies without question because existing caselaw at the time of the search established, at most, that reasonable suspicion was required to search Mr. Kamaldoss's electronic devices, and CBP agents had reasonable suspicion that his devices contained evidence of international drug trafficking. Govt. Br. at 48-49. The government does not attempt to answer the question posed in Mr. Kamaldoss's opening brief as to how a reasonable CBP officer could possibly believe that, following *Riley*, he or she was authorized to conduct a warrantless forensic search of a cell phone or laptop at the border. Appellant's Br. at 40. To apply the good faith exception in this circumstance, when a binding decision of the United State Supreme Court undermines the presumed constitutionality of a questioned practice, and no panel of this Court has ever addressed the lawfulness of that practice, would create the perverse result of incentivizing law enforcement officials to disregard

travelers' constitutional rights in arguably close cases. *See Davis v. United States*, 564 U.S. 229, 250 (2011) (Sotomayor, *J.*, concurring) ("As we previously recognized in deciding whether to apply a Fourth Amendment holding retroactively, when police decide to conduct a search or seizure in the absence of case law (or other authority) specifically sanctioning such action, exclusion of the evidence obtained may deter Fourth Amendment violations") (citing *United States v. Johnson*, 457 U.S. 537, 561 (1982)); *accord United States v. Ganias*, 824 F.3d 199, 238 (2d Cir. 2016) (*en banc*) (Chin, *C.J.*, dissenting) ("[E]ven if the warrant and our precedent were unclear as to what was allowed, the answer was not for agents to venture alone into uncharted constitutional territory").

Application of the good faith exception would also foreclose judicial review of this important Fourth Amendment question. This issue continues to present itself in this Circuit, which is home to JFK, one of the busiest airports in the United States for international travel. Mr. Kamaldoss respectfully urges this Court to decide the issue that has divided other

Courts of Appeals and to require CBP to conform the exercise of its border search authority to the Fourth Amendment's strictures.

E. ***Any Error Was Not Harmless***

The government additionally argues that even if suppression was required, any error was harmless in light of the other evidence of Mr. Kamaldoss's drug trafficking presented at trial. The government, however, placed particular emphasis on the evidence that was taken from Mr. Kamaldoss's cell phone throughout the trial, including in its closing argument to the jury, when it explained that incriminating WhatsApp messages "were taken from the defendant's phone when he was searched at JFK." SUA-476.[2] "These WhatsApp messages really are remarkable," the government told the jury, because "[t]hese messages were taken from the defendant's own phone and they're full, and I mean full, of explicit communications about drugs." *Id.* The government devoted several pages of its summation to quoting from and explaining the significance of these

[2] "SUA" refers to Mr. Kamaldoss's Supplemental Appendix, filed concurrently with the instant brief.

messages retrieved from Mr. Kamaldoss's phone, *see* SUA-476–80, SUA-486–87, and argued that the messages also corroborated Mr. Kamaldoss's use of a certain email address that the government had argued belonged to him. *See* SUA-476–77. The reliance that the government placed on the communications from Mr. Kamaldoss's phone should preclude this Court from finding their admission harmless. *See, e.g.*, *United States v. Taylor*, 745 F.3d 15, 27 (2d Cir. 2014) (wrongful admission of defendant's confession not harmless when, *inter alia*, "[t]he prosecution emphasized Taylor's confessions throughout trial, including at opening and closing").

Moreover, in making its harmless error argument, the government relies heavily on the testimony of a confidential informant, Tony Parameswaran, as well as that of a co-conspirator, Harpreet Singh. The government describes Mr. Parameswaran's testimony regarding his observations of the warehouse where Mr. Kamaldoss allegedly received drug orders but neglects to note that Mr. Parameswaran also testified that he only dealt with Mr. Navaratnarajah, Mr. Kamaladoss's co-defendant, and acknowledged that he did not have any relationship with Mr. Kamaldoss.

SUA-125. He even struggled to identify Mr. Kamaldoss in the courtroom. SUA-55, 124.

As for the testifying co-conspirator, Harpreet Singh, the defense exposed real credibility issues on cross-examination, including that Mr. Singh had entered into a sham marriage to obtain legal permanent resident status in the U.S., had helped others do the same, and later perjured himself when applying for U.S. citizenship, SUA-239–40, SUA-286–87, SUA-296, that he had submitted fraudulent tax returns to the IRS, SUA-272–75, and that by cooperating with the government against Mr. Kamaldoss, Mr. Singh expected to avoid prosecution for these other crimes and obtain an S-visa. *See* SUA-276, 289.

To the extent the government argues that the messages obtained from Mr. Kamaldoss's electronic devices were duplicative of communications obtained directly from third-party internet service providers (Govt. Br. at 55), the government fails to identify the overlap between such communications. Moreover, the email communications obtained directly from the third-party email service providers were procured with search

warrant affidavits that incorporated the messages improperly seized from Mr. Kamaldoss at the border. *See* SA 166–67, 216–17; *see also* SA 244 n.6.[3] The government should not be able to rely on evidence obtained from fruit of the poisonous tree to support its harmless error argument.

II. The Two-Level Sentencing Enhancement for "Mass Marketing by Means of an Interactive Computer Service" Was Imposed Without a Sufficient Factual Basis or Explanation

In his opening brief, Mr. Kamaldoss explained that the District Court's decision to apply a two-point enhancement pursuant to U.S.S.G. § 2D1.1 was unsupported by any evidence suggesting that either Mr. Kamaldoss or his co-conspirators marketed drugs on a large scale through a website or other "interactive computer service," as that term is used in the Guidelines. Appellant's Br. at 42–50. The government only underscores the point by repeating the District Court's conclusion that because certain trial evidence indicated that orders "were placed online," they were necessarily marketed via an interactive computer service. Govt. Br. at 60. The government does

[3] "SA" refers to the Sealed Appendix filed in connection with Mr. Kamaldoss's opening brief.

not respond to Mr. Kamaldoss's point that "interactive computer service" has a specific meaning defined by the Communications Act of 1934, 47 U.S.C. § 230(f)(2), and that the District Court failed to situate its conclusion in the context of this technical and legal definition.

The bottom line is that the trial evidence provided absolutely no visibility into how the pills at issue were marketed or to whom. Thus the mere fact that pills were dispersed to customers across the country, who somehow ordered them "online," is insufficient to confirm that they were marketed through an interactive computer service. At a minimum, the District Court should be required, on remand, to explain the basis for its finding that Mr. Kamaldoss or his co-conspirators marketed drugs via an "interactive computer service" by a preponderance of the evidence.

CONCLUSION

For the foregoing reasons, and those set forth in Mr. Kamaldoss's opening brief, Mr. Kamaldoss's convictions should be vacated and this Court should order the suppression of the evidence searched and seized from his cell phone and laptop at JFK on April 23, 2019. In the alternative,

the case should be remanded with instructions to the District Court to explain its basis for imposing the two-level mass marketing enhancement.

Respectfully submitted,

/s/ Brian E. Spears
Brian E. Spears
Federal Bar No. ct14240
Leslie A. Cahill
Federal Bar No. ct31242
SPEARS MANNING & MARTINI LLC
2425 Post Road, Suite 203
Southport, CT 06890
Telephone: (203) 292-9766
Facsimile: (203) 292-9682
Email: bspears@spearsmanning.com
lcahill@spearsmanning.com

Attorneys for Defendant-Appellant Ezhil Kamaldoss

CERTIFICATE OF COMPLIANCE

This document complies with the type-volume limit of Fed. R. App. P. 32(a)(7)(B), the word limit of Local Rule 32.1(a)(4) (A) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f): this document contains 4,325 words.

This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because: this document has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point font Palatino Linotype.

Dated: New York, New York
February 28, 2025