IN THE
UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 25-4239

UNITED STATES OF AMERICA,

Appellee,

v.

JOSE BELMONTE CARDOZO,

Appellant.

Appeal from the United States District Court
for the Eastern District of Virginia
at Alexandria
The Honorable Leonie M. Brinkema, District Judge

CORRECTED BRIEF OF THE UNITED STATES

Lindsey Halligan
United States Attorney
Special Attorney

Todd W. Blanche
Deputy Attorney General

Robert K. McBride
First Assistant United States Attorney

Lauren Halper
James Reed Sawyers
Jacqueline R. Bechara
Assistant United States Attorneys

2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700

Attorneys for the United States of America

Table of Contents

Page

Table of Authorities iii

Introduction 1

Issue Presented 3

Statement of the Case 3

A. Belmonte entices girls as young as nine years old to send him child sexual abuse material on Snapchat. 3

B. A customs officer flags Belmonte for secondary inspection based on his suspicious payment to a minor and travel from a country known for sexual exploitation of children. 5

C. The officer finds child sexual abuse material within two minutes of beginning a manual search of Belmonte's iPhones. 6

D. The district court denies Belmonte's motion to suppress, finding that the officer had reasonable suspicion and acted in good faith. 9

E. Belmonte enters a conditional guilty plea and the district court imposes a below-Guidelines sentence of 216 months. 11

Summary of Argument 12

Argument 13

The district court did not err in denying Belmonte's motion to suppress. 14

A. Manual border searches of electronic devices do not require reasonable suspicion. 14

1. This Court's binding precedent permits manual border searches of electronic devices without reasonable suspicion. 15

2. The officer's request for Belmonte's password is immaterial to the border search analysis. 27

3. Amici's novel arguments are not properly before the court and meritless. 33

B. Regardless, Belmonte's suspicious payment and travel from a country known for child exploitation established reasonable suspicion to search his phones. 35

C. At a minimum, the CBP officer acted in good faith reliance on precedent permitting manual border searches of electronic devices without reasonable suspicion. 45

Conclusion 49

Statement Regarding Oral Argument 50

Certificate of Compliance 50

Table of Authorities

Cases **Page**

Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir. 2021) 21, 25, 34

Carpenter v. United States, 585 U.S. 296 (2018) 19, 21, 34, 35, 46

Florence v. Bd. of Chosen Freeholders, 566 U.S. 318 (2012) 28

Gibbons v. Gibbs, 99 F.4th 211 (4th Cir. 2024) 23, 27

Gillespie v. United States Steel Corp., 321 F.2d 518 (6th Cir. 1963) 23

Herring v. United States, 555 U.S. 135 (2009).....45

Hudson v. Michigan, 547 U.S. 586 (2006) 45

Illinois v. Andreas, 463 U.S. 765 (1983) 29, 46

Illinois v. Lidster, 540 U.S. 419 (2004) 25

Illinois v. Wardlow, 528 U.S. 119 (2000).....35

Kansas v. Glover, 589 U.S. 376 (2020).....35

Kyllo v. United States, 533 U.S. 27 (2001).....26

Leiman v. Smith, 867 F.3d 487 (4th Cir. 2017) 33

Navarette v. California, 572 U.S. 393 (2014) 35, 38, 39

New York v. Ferber, 458 U.S. 747 (1982) 27

Paroline v. United States, 572 U.S. 434 (2014) 27

Pittston Co. v. United States, 199 F.3d 694 (4th Cir. 1999).....22

Riley v. California, 573 U.S. 373 (2014) 16, 19, 23, 28, 35

Snyder v. Phelps, 580 F.3d 206 (4th Cir. 2009).....33

United States v. Aigbekaen, 943 F.3d 713 (4th Cir. 2019) ..... passim

United States v. Arnold, 523 F.3d 941 (9th Cir. 2008).....34

United States v. Arvizu, 534 U.S. 266 (2002).....35

United States v. Bilir, 592 F.2d 735 (4th Cir. 1979).....15

United States v. Cano, 934 F.3d 1002 (9th Cir. 2019) 21, 23

United States v. Castillo, 70 F.4th 894 (5th Cir. 2023) 21, 30

United States v. Cortez, 449 U.S. 411 (1981).....35

United States v. Cortez-Rocha, 394 F.3d 1115 (9th Cir. 2005).....30

United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013)..... 31, 37, 40

United States v. Ebert, 61 F.4th 394 (4th Cir. 2023).....37

United States v. Flores-Montano, 541 U.S. 149 (2004) 15, 24, 28

United States v. Foreman, 369 F.3d 776 (4th Cir. 2004) 41

United States v. Foster, 824 F.3d 84 (4th Cir. 2016).....38

United States v. Gavegnano, 305 F. App'x 954 (4th Cir. 2009) (unpublished) (per curiam).....32

United States v. Grogins, 163 F.3d 795 (4th Cir. 1998).....35

United States v. Hill, 849 F.3d 195 (4th Cir. 2017)..... 45, 48

United States v. Hunt, 123 F.4th 697 (4th Cir. 2024)..... 18, 19, 22

United States v. Ickes, 393 F.3d 501 (4th Cir. 2005)..... passim

United States v. Jones, 952 F.3d 153 (4th Cir. 2020).....29

United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018) ..... passim

United States v. Krueger, 145 F.4th 460 (4th Cir. 2025).....37

United States v. Linarez–Delgado, 259 F. App'x 506 (3d Cir. 2007) (unpublished) 22

United States v. Martin, 690 F.2d 416 (4th Cir. 1982).....29

United States v. McAuley, 563 F. Supp. 2d 672 (W.D. Tex. 2008).....30

United States v. Mendez, 103 F.4th 1303 (7th Cir. 2024) 21, 25, 27, 30

United States v. Montoya de Hernandez, 473 U.S. 531 (1985)..... 15, 34

United States v. Ninsawat, No. 24-1276, 2025 WL 1217385 (6th Cir. Apr. 28, 2025) 36

United States v. Nkongho, 107 F.4th 373 (4th Cir. 2024) ..... passim

United States v. Nutter, 137 F.4th 224 (4th Cir. 2025).....33

United States v. Ojedokun, 16 F.4th 1091 (4th Cir. 2021) 41

United States v. Oloyede, 933 F.3d 302 (4th Cir. 2019).....33

United States v. Perkins, 363 F.3d 317 (4th Cir. 2004)..... passim

United States v. Pratt, 915 F.3d 266 (4th Cir. 2019).....25

United States v. Qin, 57 F.4th 343 (1st Cir. 2023) 20, 31

United States v. Quarles, No. 23-10377, 2025 WL 1430866 (11th Cir. May 19, 2025) 30

United States v. Ramsey, 431 U.S. 606 (1977).....15

United States v. Ross, 456 U.S. 798 (1982).....29

United States v. Saboonchi, 990 F. Supp. 2d 536 (D.Md. 2014)..... 25, 30

United States v. Sanders, 107 F.4th 234 (4th Cir. 2024).....37

United States v. Smart, 91 F.4th 214 (4th Cir. 2024) 40

United States v. Stephens, 764 F.3d 327 (4th Cir. 2014)..... 45, 47, 48

United States v. Stewart, 729 F.3d 517 (6th Cir. 2013).....22

United States v. Taylor, 54 F.4th 795 (4th Cir. 2022) 46

United States v. Taylor-Sanders, 88 F.4th 516 (4th Cir. 2023).....31

United States v. Thirty–Seven (37) Photographs, 402 U.S. 363 (1971).....20

United States v. Touset, 890 F.3d 1227 (11th Cir. 2018) 20, 22, 37, 40

United States v. Wanjiku, 919 F.3d 472 (7th Cir. 2019).....40

United States v. Xiang, 67 F.4th 895 (8th Cir. 2023) 20, 21

Statutes

18 U.S.C. § 2251(a) 9

18 U.S.C. § 2252(a)(1).....9

18 U.S.C. § 2422(b) 9

Other Authorities

Compelled Decryption and the Privilege Against Self-Incrimination, 97 Tex. L. Rev. 767 (2019).....32

U.S. Customs & Border Prot., *Border Search of Electronic Devices* (2018), https://perma.cc/U33A-8E8S 17

U.S. Customs & Border Prot., *Border Search of Electronic Devices Tear Sheet* (2023), https://perma.cc/F8DN-BNAZ.....47, 48

U.S. Customs & Border Prot., CBP Directive No. 3340-049A, *Border Search of Electronic Devices* (January 4, 2018), https://perma.cc/KCL3-U3RA.....7

U.S. Dep't of State, *Trafficking in Persons Report* (2023), https://perma.cc/DVR8-QV2D 43

U.S. Dep't of State, *Trafficking in Persons Report: Bolivia* (2023), https://perma.cc/6HZS-MPCM.....6, 42

U.S. Dep't of State, *Trafficking in Persons Report: Bolivia* (2024), https://perma.cc/LSC6-DCFP.....43

Introduction

For at least three years, Jose Belmonte Cardozo ("Belmonte") tricked, manipulated, and enticed girls as young as nine years old to create and send him sexually explicit images and videos of themselves on Snapchat. He employed various schemes to obtain child sexual abuse material ("CSAM") from his victims, including convincing a 15-year-old girl that he was a teenage boy and that they were in a relationship. When Belmonte received CSAM from his victims, he would surreptitiously record it and save the material to a password-protected hidden folder on his cell phone. Ultimately, Belmonte exploited at least six, and potentially as many as 78, minor victims, and amassed a collection of more than 1,000 images and videos depicting children engaged in sexually explicit conduct.

In May 2024, U.S. Customs and Border Protection ("CBP") received information from a mobile payment application that Belmonte had engaged in a suspicious financial transaction with a minor indicative of the purchase of CSAM. When CBP learned that Belmonte was flying to Dulles International Airport ("Dulles") from Bolivia—a high risk country for child sex trafficking—a CBP officer placed a lookout for him to be referred to secondary inspection. Once there, CBP conducted a brief, manual inspection of Belmonte's two cell phones, discovering CSAM in a hidden folder within two minutes. Belmonte was

subsequently charged with offenses related to online sexual exploitation of children and CSAM.

Belmonte moved to suppress, contending that the manual border search of his phones required reasonable suspicion, which he claimed CBP did not have. The district court denied the motion, concluding that the CBP officer had reasonable suspicion based on Belmonte's suspicious financial transaction and his travel from a country considered to be high risk for child sex trafficking. Alternatively, the court found the good faith exception would preclude suppression. Belmonte then entered a conditional guilty plea preserving his right to appeal the denial of his motion to suppress.

The district court properly denied Belmonte's motion to suppress. For one, this Court has squarely held that manual border searches of electronic devices do not require "reasonable suspicion." *United States v. Ickes*, 393 F.3d 501, 507 (4th Cir. 2005). A panel decision remains binding unless it is impossible to reconcile with a subsequent en banc or Supreme Court decision. *Ickes* is perfectly consistent with subsequent Supreme Court decisions, as all five circuit courts to address the issue have held. *Ickes* thus remains good law and resolves this case.

Alternatively, the district court did not err in finding reasonable suspicion based on the report flagging Belmonte's suspicious transaction with a minor suggestive of the purchase of CSAM and his travel from a country associated with

child sexual exploitation. At an absolute minimum, the officer acted in good faith reliance on *Ickes*.

Issue Presented

Whether the district court erred in denying Belmonte's motion to suppress based on the manual inspection of his cell phones at the border.

Statement of the Case

A. Belmonte entices girls as young as nine years old to send him child sexual abuse material on Snapchat.

From May 2021 through May 2024, Jose Belmonte Cardozo used Snapchat to find minor girls and entice them to create and send him images and videos of themselves engaged in sexually explicit conduct. JA264. Belmonte employed multiple Snapchat accounts as part of his scheme and tailored his approach to each victim. *See, e.g.*, JA264-267. All told, law enforcement discovered a total of 78 potential minor victims, 16 of whom have been identified. *See* ECF No. 56-1 at 3.

With some victims, Belmonte posed as a teenaged boy and pretended to initiate a romantic relationship. *See, e.g.*, JA265-266. For instance, he told one 15-year-old victim he was a high school student in Florida named "Justin" and sent her pictures of an adolescent boy. JA265-266. Over the course of several months, Belmonte spoke with the victim by phone and invented elaborate "stories" about his fictional life. JA291-292. Among other fabulations, he claimed that his "mom and dad were having relationship problems" and said that he "got a new dog, but his

mom wouldn't let him keep the dog in his room." JA291-292. Once Belmonte won the victim's trust, he pushed her to send him sexually explicit images and videos—which she did because she "really liked" "Justin." JA266, JA291. Indeed, so deep was the victim's trust that she attempted to mail "Justin" a card to "to ask him to be my valentine" and confided that she had previously been raped. JA292. Belmonte responded that the rape was her "fault" and that he could not "trust [her] anymore because" she "just let it happen." JA292.

With other victims, Belmonte claimed he would grant them access to an exclusive chat group if they passed a series of tests, including sending him sexually explicit videos of themselves. JA264, JA266-267. Belmonte used that approach to exploit two girls, aged 11 and 9, who were sharing a Snapchat account. JA266. To "prove you're freaky enough to be added" to the group chat, Belmonte demanded "a snap video of your 😈 [*i.e.*, vagina] pls like spread it open," which the girls provided. JA266.

After receiving images and videos from his victims through Snapchat, Belmonte used a second iPhone to photograph or record the material. JA265. Doing so prevented the minors from receiving a notification in Snapchat that their images or videos had been saved. JA265. Belmonte then stored the material in his iPhones' "hidden folder" (a password-protected folder not immediately visible when viewing an iPhone's saved photographs). JA265; *see* JA42, JA110.

B. A customs officer flags Belmonte for secondary inspection based on his suspicious payment to a minor and travel from a country known for sexual exploitation of children.

In 2024, Sara Oliphant served as a CBP Port Intelligence Officer at Dulles International Airport. JA145. At Dulles, Oliphant was "focus[ed] solely on child sexual abuse material," "human trafficking[,] and child sex tourism[.]" JA145. In that role, Oliphant reviewed and analyzed trends related to CSAM, human trafficking, and child sex tourism to interdict contraband and apprehend violators at the U.S. border. JA145. In May 2024, CBP conducted a special operation focused on CSAM and child sex trafficking. JA148-149. During that operation, Officer Oliphant received a report shared by CBP's National Targeting Center, which "screens . . . inbound and outbound passengers and cargo for any threats against the United States" and sends "leads for inspection[]" to field officers. JA147-148; *see also* JA41. The report originated with Cash App, a private payment application typically used on phones or tablets. JA155-156, JA160, JA163. Cash App flagged five users—including Belmonte—for engaging in suspicious financial transactions with minors indicative of CSAM purchases. JA149, JA155-156, JA160, JA163-164. The Cash App report covered the users' transactions from February to June 2023 and noted that at least one included "Snap" in the memo line. JA156-158, JA162.

Based on her training and experience, Officer Oliphant knew that "Snap" was likely shorthand for Snapchat, where CSAM was "frequently" and "heavily"

"elicited" from minor victims. JA162. Officer Oliphant also observed that Belmonte was traveling to Dulles from Bolivia, by way of Colombia. JA149. This was significant to Officer Oliphant, because she knew based on her review of a State Department report and independent "research" that Bolivia was "a high-risk country for child sex tourism and [CSAM]." JA147, JA70; *see* U.S. Dep't of State, *Trafficking in Persons Report: Bolivia* (2023), https://perma.cc/6HZS-MPCM. Based on the Cash App report and Belmonte's travel from Bolivia, Officer Oliphant decided to conduct a manual border inspection of his electronic devices upon his arrival at Dulles. JA150, JA158-159; *see* JA69.

C. The officer finds child sexual abuse material within two minutes of beginning a manual search of Belmonte's iPhones.

After Belmonte's flight arrived at Dulles, he was sent to secondary inspection. JA70-71, JA150. There, Officer Oliphant located several electronic devices in Belmonte's possession, including two iPhones, and provided a "tear sheet" outlining CBP's border search authority related to electronic devices. JA70-71, JA150, JA160-161; *see* JA120-121 (tear sheet). The tear sheet notes that travelers "are obligated to present electronic devices . . . in a condition that allows for the examination of the device and its contents" and that "[f]ailure to assist CBP in accessing the electronic device and its contents for examination may result in the detention of the device in order to complete the inspection." JA120.

Officer Oliphant asked Belmonte to provide his passcode and unlock the devices, which he did. JA161. She then asked him to sit in a waiting area outside. JA71. When he exited the inspection area, Belmonte left the tear sheet on the inspection table along with his backpack. JA71.

Before beginning her manual review, Officer Oliphant placed the two iPhones in airplane mode. JA161. Doing so ensures that officers cannot access information not stored on the device. *See* U.S. Customs & Border Prot., CBP Directive No. 3340-049A, *Border Search of Electronic Devices* (January 4, 2018), https://perma.cc/KCL3-U3RA. Officer Oliphant looked first for a hidden folder in the phones' Photo gallery, where she knew offenders often hide CSAM. JA161. Within two minutes of her search of both iPhones, she found several images and videos in the hidden folder that appeared to depict children engaged in sexually explicit conduct. JA162; *see* JA71.

Officer Oliphant alerted her supervisor and agents with Homeland Security Investigations ("HSI"), who performed their own manual searches of Belmonte's phones. JA14, JA43, JA71. Officer Oliphant and an HSI agent then attempted to interview Belmonte. JA71. After waiving his *Miranda* rights, Belmonte initially claimed that Officer Oliphant never told him she planned to search his electronic devices or gave him a tear sheet. JA71. Belmonte was again informed of CBP's border search authority and provided with another copy of the tear sheet. JA71.

Another officer who witnessed the original interaction also confirmed that Belmonte had been provided with a tear sheet and had "willingly turned over his devices." JA71. After that gambit failed, Belmonte acknowledged his actions, which he called a "mistake." JA72. Later that evening, Belmonte twice told an agent escorting him to jail that he was "'sorry you guys had to look at that stuff' on his iPhone." JA17.

The day after Belmonte's arrest, an HSI computer forensic agent conducted a full forensic search of his iPhones using a specialized forensic tool (Graykey) to extract the full contents of each device and specialized software (Axiom) to process the raw, extracted data. JA44-45. The forensic search enabled the agent to view data not accessible through a manual search, such as deleted files and files in unallocated space. JA44-45. The forensic search ultimately uncovered more than 600 images and videos depicting minors engaged in sexually explicit conduct. JA45. Many of the CSAM files appeared to originate from Snapchat and one had been captured only three days before Belmonte's arrest. JA45. A subsequent search of Belmonte's Virginia home, pursuant to a search warrant, revealed 500 additional images and videos depicting child sexual abuse, including CSAM elicited through Snapchat, dating back to 2021. JA268.

D. The district court denies Belmonte's motion to suppress, finding that the officer had reasonable suspicion and acted in good faith.

The day after Belmonte's arrest, in May 2024, the government charged him by complaint with a single count of transporting child pornography, in violation of 18 U.S.C. § 2252(a)(1), (b)(l). JA10. By mid-June, the government had provided initial discovery, including Officer Oliphant's report summarizing the border search. *See* JA75-76; JA68-73 (report).

As the investigation progressed and the government identified Belmonte's victims, the grand jury issued a series of indictments. JA18-24. In September 2024, the grand jury ultimately returned a ten-count second superseding indictment, charging Belmonte with five counts of sexual exploitation of a child, in violation of 18 U.S.C. § 2251(a), (e); two counts of coercion and enticement of a minor, in violation of 18 U.S.C. § 2422(b); and one count each of transportation, receipt, and possession of CSAM, in violation of 18 U.S.C. § 2252(a)(1), (a)(2), (a)(4)(B), (b)(1), (b)(2). JA90-102.

Belmonte moved to suppress "[a]ll the evidence in this case," contending that manual border searches of electronic devices require reasonable suspicion, which Officer Oliphant purportedly lacked. JA25-39. Belmonte neither claimed that his phones' encryption altered the Fourth Amendment analysis nor raised a Fifth Amendment compelled-disclosure argument. *See generally* JA25-39. In his reply

brief, Belmonte asserted for the first time that entering an iPhone's password results in its "decrypt[ion]," which he said transformed the search into a non-routine one requiring reasonable suspicion. *See, e.g.*, JA81, JA85-86. Again, Belmonte did not raise a Fifth Amendment argument. *See generally* JA77-89. Later, Belmonte submitted a declaration from a proposed forensic expert and a copy of CBP's standard "tear sheet." JA106-118 (declaration); JA119-121 (tear sheet). Belmonte claimed the tear sheet was relevant to rebutting the government's assertion that he "had 'voluntarily' provided CBP the passcodes to his phones" but, again, did not advance a Fifth Amendment argument. JA103-105 & n.2. The government, in turn, asserted that Belmonte's late-breaking arguments were forfeited and, alternatively, offered the testimony of its own forensic expert. JA122-124.

The district court began the suppression hearing by stating that it did not "need" to hear from the forensic witnesses because the technical details were not "relevant." JA144, JA164. After hearing testimony from Officer Oliphant, JA144-164, the court denied the motion to suppress, JA164-169. The court reasoned that it did not "have to get into" whether manual searches require reasonable suspicion because "the evidence in this case" established it. JA166, JA168. On that score, the court first noted Officer Oliphant's knowledge that Belmonte "was coming from a country that does have some connection with child sex trafficking and child sex tourism." JA166. While "that fact alone would not have been enough," the

"confluence" of Belmonte's departure from Bolivia with the "alert" linking him to suspected child sexual exploitation was "enough to establish . . . individualized suspicion." JA167. The court also noted that, "unconnected to targeting" Belmonte, CBP focused on CSAM interdiction in May 2024. JA167.

Turning from the permissibility of the manual search to the manner in which Officer Oliphant carried it out, the court emphasized that she found CSAM within "two minutes," "went right to photos first and then the hidden photos," and did not "rummage[] through the entire phone." JA167, JA169. After finding CSAM, the court made clear, officers had more than sufficient suspicion to conduct the subsequent forensic search. JA167-168. The forensic search, too, was reasonably conducted because it was completed within a day of Belmonte's arrest. JA168-169.

Alternatively, "[e]ven if" Officer Oliphant lacked "reasonable suspicion," the court found the good faith exception precluded suppression by analogy to this Court's decision in *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018). JA169.

E. Belmonte enters a conditional guilty plea and the district court imposes a below-Guidelines sentence of 216 months.

Belmonte subsequently entered a conditional guilty plea to all ten counts of the second superseding indictment, preserving his right to appeal the denial of his motion to suppress. JA209, JA217.

Prior to sentencing, the United States Probation Office prepared a presentence investigation report describing the impact of Belmonte's exploitation on the minor

victims. *See* JA290-311. The mother of one victim, for example, reported that Belmonte "shattered my daughter's life and inflicted pain that no family should ever endure." JA290. Consequently, her daughter was "hospitalized for self-harm" and "[e]very day feels like a struggle for survival for her." JA290. The mother of another victim reported that her daughter kept asking "'Mom will he be able to find me?'" JA296. The mother could respond only "no baby girl he is put away but not sure for how long." JA296.

At sentencing in April 2025, the district court varied downward from the Guidelines range of life imprisonment and imposed a 216-month sentence. JA242, JA282. This appeal followed.

Summary of Argument

The district court did not err in denying Belmonte's motion to suppress. The brief, manual inspection of his cell phones at the border was a lawful exercise of the government's border search authority, which dates back to the nation's founding and is rooted in the sovereign's right to control who and what may enter the country. Applying that venerable authority, this Court in *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005), made clear that manual searches of electronic devices at the border do not require reasonable suspicion. This panel remains bound by that holding, which is fully consistent with subsequent Supreme Court decisions, as every other circuit to address the issue has found.

Alternatively, even if this Court decides that reasonable suspicion is required for the manual inspection of a cell phone at the border, the district court properly found that law enforcement had it in this case. Cash App's report flagging Belmonte (and four other users) for suspicious transactions with minors suggestive of the purchase of CSAM provided reasonable suspicion that Belmonte's phones contained CSAM. The report's reference to Snapchat, a mobile app known for the elicitation of CSAM, bolstered that suspicion. Moreover, Belmonte's travel from Bolivia, a country associated with child sex tourism, further supported the officer's reasonable suspicion.

At the least, suppression is not warranted because the officer acted in good faith reliance on *Ickes*. Accordingly, this Court should affirm the judgment of the district court.

Argument

In evaluating an appeal regarding the suppression of evidence, this Court reviews the district court's factual findings for clear error and its legal conclusions de novo. *United States v. Perkins*, 363 F.3d 317, 320 (4th Cir. 2004). Because the district court denied the suppression motion, this Court views the relevant facts in the light most favorable to the government. *Id.*

The district court did not err in denying Belmonte's motion to suppress.

The district court properly denied Belmonte's suppression motion for three independent reasons. First, this Court's binding precedent (and that of every other circuit to address the issue) permits manual border searches of electronic devices without reasonable suspicion. Alternatively, the Cash App report flagging Belmonte and four other users for suspicious financial transactions with minors suggestive of CSAM purchases and his travel from a country associated with child sexual exploitation established reasonable suspicion. Officer Oliphant, at a minimum, acted in good faith reliance on precedent.[1]

A. Manual border searches of electronic devices do not require reasonable suspicion.

This Court's binding holding that manual border searches of electronic devices do not require "reasonable suspicion" squarely resolves this case. *Ickes*, 393 F.3d at 507. As five other courts of appeals have recognized, that holding is perfectly consistent with the Supreme Court's subsequent cases. Nor can Belmonte escape *Ickes* through his focus on whether his phone was encrypted and Officer Oliphant's request for his password—details which no case cited by Belmonte finds relevant to the border search inquiry. Finally, the novel arguments advanced by amici (that the

[1] While officers performed subsequent manual and forensic searches after discovering CSAM in Belmonte's phones, he challenges only the initial, manual search. *See* Def. Br. 25.

First and Fourth Amendments require probable cause and a warrant) are waived and meritless.

1. This Court's binding precedent permits manual border searches of electronic devices without reasonable suspicion.

The government's border search authority dates to the nation's founding and is rooted in the sovereign's right to control "who and what may enter the country." *United States v. Ramsey*, 431 U.S. 606, 620 (1977). Since the earliest days of the republic, border searches "have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside." *Id.* at 619. Congress "granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country." *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). Indeed, the "same Congress which proposed the Fourth Amendment" also enacted the first far-reaching customs statute. *Ramsey*, 431 U.S. at 616-17. This Court too has long recognized the "'primordial' national interest in protecting the borders against violation by illegal importations." *See, e.g.*, *United States v. Bilir*, 592 F.2d 735, 739 (4th Cir. 1979). Despite those weighty interests, the Supreme Court has recognized that certain "highly intrusive," "nonroutine border searches such as strip, body-cavity, or involuntary x-ray searches" may require "some level of suspicion."

United States v. Flores-Montano, 541 U.S. 149, 152 (2004); *Montoya de Hernandez*, 473 U.S. at 541 n.4.

This Court applied those principles to manual border searches of electronic devices in *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005). There, the Court weighed the "greater interest on the side of the government at the border" against the "lesser interest on the side of the potential entrant." *Id.* at 506. On one hand, manual searches of digital devices further the government's "'paramount interest in protecting[] its territorial integrity'" and "prevent[ing] 'the introduction of contraband'"—from "child pornography" to "terrorist plans"—"'into this country.'" *Id.* at 505-07. On the other, "[s]ince 'a port of entry is not a traveler's home,' his expectation of privacy there is substantially lessened." *Id.* The Court thus held that manual border searches of electronic devices fall on the "routine" side of the line and do not require "reasonable suspicion." *Id.* at 505, 507.

A decade later, this Court addressed "forensic" or "advanced" border searches, *i.e.*, those involving "the connection of external equipment" to extract and analyze a digital device's contents. *United States v. Kolsuz*, 890 F.3d 133, 146 n.6 (4th Cir. 2018). Relying on *Riley v. California*, 573 U.S. 373 (2014), which held that the search incident to arrest exception does not apply to searches of cell phones, this Court distinguished forensic and manual searches. *Kolsuz*, 890 F.3d at 144-46. In doing so, the Court emphasized the "sheer quantity of data stored on

smartphones" which—"[s]ubjected to comprehensive forensic analysis" and "analyzed cumulatively"—could "reveal an unparalleled breadth of private information." *Id.* There, the forensic search "reveal[ed] 896 pages' worth of sensitive data including personal contacts, photographs, web browsing history, and a 'history of [Kolsuz's] physical location down to precise GPS coordinates.'" *Id.* at 145. Consequently, *Kolsuz* required "some form of individualized suspicion" for a forensic border search, although it left open whether reasonable suspicion would suffice, or probable cause was required. *Id.* at 146.

In distinguishing forensic from manual searches, *Kolsuz* made clear that it had "no occasion to consider" whether *Ickes*' holding permitting "suspicionless manual searches of digital devices at the border" had been "call[ed] into question" by *Riley*. 890 F.3d at 141, 146 n.5. To the contrary, *Kolsuz* favorably described a recently adopted CBP policy (still in effect today) requiring reasonable suspicion for forensic searches but permitting manual searches without it. *Id.* at 146 & n.6 (citing U.S. Customs & Border Prot., *Border Search of Electronic Devices* 4-5 (2018), https://perma.cc/U33A-8E8S). The CBP policy, the Court explained, demonstrates that "the distinction between manual and forensic searches is a perfectly manageable one" and "that treating forensic phone searches as nonroutine need not interfere unduly with the agency's protective mission at the border." *Id.*

A year after *Kolsuz*, this Court held that the suspicion required for a forensic border search must be suspicion of digital contraband or evidence of a transnational crime, rather than a mere "domestic crime." *United States v. Aigbekaen*, 943 F.3d 713, 721-23 (4th Cir. 2019).

Finally, in *United States v. Nkongho*, this Court held that the same standard that applies to a nonroutine forensic border search must also apply to "the nonroutine seizure of a phone for the purpose of a forensic search[.]" 107 F.4th 373, 381-82 (4th Cir. 2024). Again, the Court left open the degree of suspicion required for a forensic search or nonroutine seizure but the Court flatly rejected a "warrant" requirement, recognizing that border searches of digital devices "are critical for preventing cross-border crime and the importation of contraband"—"such as child pornography." *Id.* at 381-84 & n.3.

The progression of this Court's border-search caselaw makes clear that it has never purported to overrule *Ickes*'s holding that manual border searches of digital devices do not require reasonable suspicion, which remains good law and resolves this case. "'[A] panel of this court is bound by prior precedent from other panels' and may not overturn prior panel decisions unless there is 'contrary law from an en banc or Supreme Court decision.'" *United States v. Hunt*, 123 F.4th 697, 702 (4th Cir. 2024). The Court does "'not lightly presume that the law of the circuit has been overturned.'" *Id.* "Instead, '[a] Supreme Court decision overrules or abrogates [this

Court's] prior precedent only if [this Court's] precedent is impossible to reconcile with' that decision." *Id.* "'If it is possible for [this Court] to read [its] precedent harmoniously with Supreme Court precedent, [it] must do so.'" *Id.* Here, *Ickes* is fully consistent with *Riley*—or, at the very least, not "'impossible to reconcile with'" it—and thus continues to bind the Court. *See id.*; *contra* Def. Br. 46.

In *Riley*, the Supreme Court declined to extend the search incident to arrest exception to cellphones because the doctrine's justifications—officer safety, the potential destruction of evidence, and the arrestee's reduced privacy interests—were not applicable to cellphone searches. 573 U.S. at 386-98. The Court adopted similar reasoning in *Carpenter v. United States*, 585 U.S. 296 (2018), a case Belmonte mentions but does not argue abrogated *Ickes*. Def. Br. 23-24. *Carpenter* declined to extend the third-party doctrine because the "rationale[s] underlying" it—"voluntary exposure" and the "limited" nature of the information—were similarly inapplicable to historical cell-site location information. 585 U.S. at 313-16.

By contrast with *Riley* and *Carpenter*, the border search justifications—the government's "'paramount interest in protecting its territorial integrity'" and "prevent[ing] 'the introduction of contraband'" and a traveler's reduced "expectation of privacy" at the border—apply with equal force to electronic devices. *Ickes*, 393 F.3d at 506. This Court reaffirmed as much only last year, recognizing that "searching a traveler's electronic devices may be vital to promoting" the

government's "paramount" "interests at the border"—"preventing cross-border crime and the importation of contraband." *Nkongho*, 107 F.4th at 381-82. On the other side of the ledger, *Nkongho* likewise recognized that, despite the "ubiquity of smartphones" and the "privacy interests at stake," "a traveler has a diminished expectation of privacy at the border." *Id.*

The scourge of CSAM underscores that the government's interest in stopping contraband on the border does not depend on whether it takes the form of digital files or physical photographs. Historically, "[c]ustoms officers" enjoyed "[un]questioned" authority to "inspect" a traveler's physical "luggage" to interdict CSAM or other "obscene" "photographs." *See United States v. Thirty–Seven (37) Photographs*, 402 U.S. 363, 365-66, 376-77 (1971). Today, "child pornography offenses overwhelmingly involve the use of electronic devices for the receipt, storage, and distribution of unlawful images." *United States v. Touset*, 890 F.3d 1227, 1235-36 (11th Cir. 2018). Thus, to except digital devices from the government's manual border search authority would "create a special rule that will benefit offenders who now conceal contraband in a new kind of property." *Id.* at 1236.

Nor is CSAM the only contraband or evidence of transnational crime malefactors seek to smuggle in or out of the nation on electronic devices. From "trade secrets" being conveyed to a foreign adversary, *United States v. Xiang*, 67

F.4th 895, 899 (8th Cir. 2023), "evidence" of illegal exportation to "a Chinese university with military ties," *United States v. Qin*, 57 F.4th 343, 345 (1st Cir. 2023), or "plan[s] to ship" "stolen" "military equipment to Mexico," the government's interests in searching digital devices at the border remains "paramount," *Nkongho*, 107 F.4th at 383. "If anything, the advent of sophisticated technological means for concealing contraband only heightens the need of the government to search property at the border." *United States v. Mendez*, 103 F.4th 1303, 1309 (7th Cir. 2024).

Unsurprisingly, then, every court of appeals to address the issue has held that *Riley* does not undercut the justifications for manual border searches of electronic devices without reasonable suspicion. *See, e.g.*, *Alasaad v. Mayorkas*, 988 F.3d 8, 17-19 (1st Cir. 2021) ("*Riley*'s . . . privacy concerns . . . are nevertheless tempered by the fact that the searches are taking place at the border, where the 'Government's interest in preventing the entry of unwanted persons and effects is at its zenith,' . . . and the 'Fourth Amendment balance of interests leans heavily to the Government'"); *United States v. Castillo*, 70 F.4th 894, 897-98 (5th Cir. 2023) ("when it comes to manual cell phone searches at the border . . . *Riley* does not require either a warrant or reasonable suspicion"); *Mendez*, 103 F.4th at 1307-10 ("*Riley* and *Carpenter* had nothing to do with the border context"); *Xiang*, 67 F.4th at 900-01 (challenge to "routine border search of electronic devices . . . 'rests on a misapprehension of the applicability' of *Riley*"); *United States v. Cano*, 934 F.3d 1002, 1015-16 (9th Cir.

2019) ("[n]or do we believe that *Riley* renders" prior holding "that manual searches of cell phones at the border are reasonable without individualized suspicion" "insufficiently protective"); *Touset*, 890 F.3d at 1233.[2] *Ickes* cannot be "impossible to reconcile" with *Riley* if five circuits (four of them without preexisting precedent) reached the same holding as *Ickes* after *Riley*. *See Hunt*, 123 F.4th at 703. *Riley* "thus provide[s] no basis for a panel to depart from this Court's previous rejection of" a reasonable suspicion requirement for manual border searches of electronic devices. *Id.* at 704.

To avoid *Ickes*, Belmonte seeks to reinvent its holding: the officers there, Belmonte claims, had "probable cause," so this Court *could have* affirmed the search on that basis without deciding whether reasonable suspicion was required. Def. Br. 46-47. *Ickes*, however, expressly declined to "enthron[e]" "reasonable suspicion[]" as the "constitutional" standard. 393 F.3d at 507. Thus, Belmonte cannot avoid *Ickes*' clear holding by claiming the Court might have been able to reach the same result on a different ground. *See Pittston Co. v. United States*, 199 F.3d 694, 703

[2] The two other circuits that addressed the issue prior to *Riley* also found manual searches of digital devices permissible without reasonable suspicion. *See United States v. Linarez–Delgado*, 259 F. App'x 506, 508 (3d Cir. 2007) (unpublished) ("Data storage media and electronic equipment, such as films, computer devices, and videotapes, may be inspected and viewed during a reasonable border search."); *United States v. Stewart*, 729 F.3d 517, 525-26 (6th Cir. 2013) ("non-forensic examination of . . . laptop computer" is a "routine border search" for which "reasonable suspicion" is not "required").

(4th Cir. 1999) (a statement is not dictum "when 'the matter was before the court . . . ; was argued before the court; and was passed upon by the court'").

For good reason, Belmonte does *not* argue there is any basis to distinguish the computer at issue in *Ickes*, 393 F.3d at 50, from the iPhones at issue here. *See* Def. Br. 46-47. *Riley* afforded cellphones heightened protection based on its recognition that they are "minicomputers." 573 U.S. at 593. And there is simply "no basis to distinguish a [border] cell phone search from a [border] laptop search." *See, e.g.*, *Cano*, 934 F.3d at 1015.

Belmonte offers several counterarguments seeking to conflate manual and forensic searches and cast doubt on the justifications for border searches of digital devices. *See* Def. Br. 22-34. This Court rejected many of his contentions in *Ickes*. *See, e.g.*, 393 F.3d at 506 (emphasizing that "practical" realities cabin manual search authority). But even to the extent that Belmonte raised a new theory that would persuade the Court were it writing on a blank slate, the Court is still bound by *Ickes*. *See Gibbons v. Gibbs*, 99 F.4th 211, 215 (4th Cir. 2024) ("Few—if any—judicial opinions reflect on and reject every conceivable counterargument, and 'the rule that one panel cannot overrule' another would be weak tea indeed if all a later panel had to do was identify a fact, theory, or argument a previous panel did not address.").

That reality aside, none of Belmonte's arguments holds water. Start with his assertion that "the search here should be deemed nonroutine" because it "implicated

every type of private information that was at issue in *Kolsuz*." Def. Br. 18. While the government and Belmonte both advocate categorical rules rather than application of a "complex balancing test[]" to the facts of his case, *see Flores–Montano*, 541 U.S. at 152, Belmonte's description of the search is simply incorrect. Officer Oliphant went "right" to his phone's "photos" app and looked for "hidden" folders (where she knew from experience exploiters store CSAM). JA161, JA169. Without "rummag[ing] through the entire phone," she found CSAM within "two minutes." JA161-162, JA169. That is a far cry from the forensic search in *Kolsuz*, which "lasted for a full month, and yielded an 896–page report that included Kolsuz's personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of Kolsuz's physical location down to precise GPS coordinates." 890 F.3d at 139.

Backpedaling from the facts (which underscore the limited nature of a typical manual search), Belmonte claims that manual searches *could* proceed "for any amount of time" and thereby "review every photo and video and word-search every written communication on a device." Def. Br. 27-29. Not so. "Even at the border . . . the government's authority is not without limits" and the "'ultimate touchstone' of the Fourth Amendment remains reasonableness.'" *Kolsuz*, 890 F.3d at 138. Thus, "a seizure reasonable at its inception must remain reasonable in scope and *duration* to satisfy the Fourth Amendment." *Id*. at 141 (emphasis added); *cf.*

Nkongho, 107 F.4th at 382 (requiring individualized suspicion for a nonroutine seizure of a phone for purposes of a forensic border search); *United States v. Pratt*, 915 F.3d 266, 272-73 (4th Cir. 2019) (holding that an unreasonable delay in completing a search can violate the Fourth Amendment).

Courts have also recognized that "[p]ractical" constraints limit the extent of manual border searches. *See Ickes*, 393 F.3d at 506. "Put simply, Customs officials do not have the time or resources—or, most likely, the inclination—to" subject travelers to extended manual searches, *see United States v. Saboonchi*, 990 F. Supp. 2d 536 at 570, (D. Md. 2014), "without any degree of suspicion," *contra* Def. Br. 34. These kinds of "[p]ractical considerations—namely, limited police resources," moreover, have often informed the permissible scope of Fourth Amendment searches. *See, e.g.*, *Illinois v. Lidster*, 540 U.S. 419, 426 (2004). These practical limitations mean that manual searches are qualitatively different than forensic searches. Given the inability to "download and peruse the phone's entire contents," *Mendez*, 103 F.4th at 1310, and need to "manually traverse the contents," *Alasaad*, 988 F.3d at 18, "a manual search . . . will never result in the human visualization of more than a fraction of the content of the device," *Saboonchi*, 990 F. Supp. 2d at 547.

Seeking to blur *Kolsuz*'s distinction between manual and forensic searches, Belmonte argues that "the use of external equipment and specialized software is

irrelevant to the Fourth Amendment inquiry." Def. Br. 27. The Supreme Court, however, has recognized that the use of "sense-enhancing technology" can alter the Fourth Amendment balance. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001); *id.* at 40 (holding that use of "thermal imaging" device on a home constitutes a Fourth Amendment search). And, in *Kolsuz*, this Court specifically found that the use of "external equipment and specialized software"—the standard adopted by the CBP policy that remains in effect today—creates a "perfectly manageable" distinction between searches requiring individualized suspicion and those that do not. *See* 890 F.3d at 146 & n.6.

Belmonte points to a few out-of-circuit district court decisions—currently on appeal to the Second Circuit—requiring "probable cause and a warrant" to conduct a manual border search. Def. Br. 28-29; *see, e.g.*, *United States v. Alisigwe,* No. 24-960 (2d Cir. argued Mar. 28, 2025). Belmonte, however, does not actually advance that outlier position, which is squarely foreclosed by this Circuit's precedent. *See Nkongho*, 107 F.4th at 384 & n.3 (rejecting warrant requirement).

Belmonte also errs in suggesting that the government's interest in interdicting CSAM at the border is limited because it "exists and travels 'in the cloud.'" *See* Def. Br. 31-32. As Belmonte's own actions demonstrate, those seeking to smuggle contraband into or out of the country often conclude they can more easily avoid detection by storing that illicit material locally on their cellphone (or another

electronic device) than by leaving a digital footprint on the internet. Thus, the reality that "digital contraband like child pornography can pass into the country electronically or be accessed remotely does little to diminish the government's interest in preventing its physical entry into the country." *Mendez*, 103 F.4th at 1309; *see also Paroline v. United States*, 572 U.S. 434, 439-40 (2014) (reiterating that "the exploitive use of children in the production of pornography has become a serious national problem" and that "the harms caused by child pornography" are "more extensive because child pornography is 'a permanent record' of the depicted child's abuse, and 'the harm to the child is exacerbated by [its] circulation.'").

2. The officer's request for Belmonte's password is immaterial to the border search analysis.

Belmonte next attempts to escape *Ickes* by focusing on whether he was required to provide his password and whether his iPhone was locked and encrypted. Def. Br. 30-31, 33-35. *Ickes*, however, permitted manual searches of digital devices without "exception" to avoid "legal wrangles at the border" and "drawing difficult lines." 393 F.3d at 506. Belmonte's encryption and password contentions are thus merely "a fact, theory, or argument a previous panel did not address," which does not suffice to escape *Ickes*' categorical holding. *See Gibbons*, 99 F.4th at 215.

In all events, locking and passwords have no bearing on the border search analysis for two additional, independent reasons: First, because Belmonte has foresworn a focus on the unique facts of his case in recognition of the Supreme

Court's rejection of complex balancing tests in the border search context. Second, because border search authority extends to locked property and devices.

The Supreme Court has repeatedly emphasized the need for "categorical rules" that "provide clear guidance to law enforcement" in the Fourth Amendment context. *Riley*, 573 U.S. at 398; *see also, e.g.*, *Florence v. Bd. of Chosen Freeholders*, 566 U.S. 318, 338 (2012) (emphasizing "'essential interest in readily administrable rules'"). For that reason, the High Court specifically rejected "[c]omplex balancing tests to determine" whether a border search is "'routine.'" *Flores–Montano*, 541 U.S. at 152. This Court likewise recognized that CBP's policy distinguishing between "basic" border searches (which do not employ "external equipment") and "advanced" border searches (which do) is "perfectly manageable." *Kolsuz*, 890 F.3d at 146 & n.6. Given that caselaw, Belmonte rightfully disclaims a focus on "the facts of this case" as "unworkable" and advocates instead for a categorical rule requiring "reasonable suspicion to search a cell phone at the border." *See* Def. Br. 20-30. His choice to avoid focusing on the specifics of the search here—which lasted only two minutes and went straight to the hidden folders where CSAM was likely to be found—means this Court need not get bogged down in the details of iPhone encryption schemes or Officer Oliphant's request for his password. *See* JA144, JA164 (recognizing that "forensic" details are "irrelevant").

In any case, whether a phone is locked or encrypted does not bear on the border search analysis. For obvious reasons, courts have long held that defendants cannot avoid otherwise permissible searches by locking their property. Hence, officers may secure a warrant to "open" a defendant's "safes or locked boxes" on the same basis as any other warrant. *See, e.g.*, *United States v. Jones*, 952 F.3d 153, 157-58 (4th Cir. 2020). Officers may search locked vehicles and open locked containers in a vehicle pursuant to the automobile exception. *See, e.g.*, *United States v. Ross*, 456 U.S. 798, 824-25 (1982); *United States v. Martin*, 690 F.2d 416, 419-21 (4th Cir. 1982). And, so long as the act of unlocking the property does not inflict significant damage, officers may search "locked" items pursuant to their "border search" authority. *Illinois v. Andreas*, 463 U.S. 765, 766-67 (1983). The Supreme Court thus took it for granted that a "[c]ustoms inspector" could "open[]" a "locked metal container" and examine the "wooden table" found inside during a "border search." *See id.* To hold otherwise would vitiate the rule that "luggage carried by a traveler entering the country may be searched at random" by drawing a nonsensical distinction between the "traveler who carries a toothbrush and a few articles of clothing in a paper bag" and "the sophisticated executive with the locked attaché case." *See Ross*, 456 U.S. at 822-83.

Hewing to the Supreme Court's guidance, the lower courts have recognized that locked spaces, containers, or luggage may likewise be unlocked, accessed, and

searched at the border pursuant to border search authority. *See, e.g.*, *United States v. Cortez-Rocha*, 394 F.3d 1115, 1119-20 (9th Cir. 2005) (holding that "cutting a spare tire" is "routine" search that does not require "reasonable suspicion" because contrary "rule" would exempt "[a]ny locked container" from border search). The same is true of locked digital devices: "[J]ust as a luggage lock does not render the contents of a suitcase immune from search, a password protected file is not unsearchable on that basis alone." *See, e.g.*, *Saboonchi*, 990 F. Supp. 2d at 560-61; *United States v. McAuley*, 563 F. Supp. 2d 672, 678 (W.D. Tex. 2008) ("A password is simply a digital lock. Locks are usually present on luggage and briefcases, yet those items are subject to 'routine' searches at ports of entry all the time.").

For his part, Belmonte proffers a few cases where courts noted that manual searches do not typically access "encrypted" files. Def. Br. 30-31. But he identifies no case finding a manual border search non-routine because an officer requested the defendant's password or the device was locked or encrypted. For good reason, as the other courts of appeals have never suggested those details are relevant to whether a border search is routine. *See, e.g.*, *Mendez*, 103 F.4th at 1305 ("Mendez gave Callison his cell phone and its passcode . . . Using the phone's passcode, Callison also opened a protected application called 'iSafe,' where he discovered more illicit images."); *Castillo*, 70 F.4th at 896 ("He also provided the passcode to unlock his cell phone to a Homeland Security Investigations special agent."); *United States v.*

Quarles, No. 23-10377, 2025 WL 1430866, at *1 (11th Cir. May 19, 2025) ("The investigators seized Quarles's and Krzeminska's cell phones. Both Quarles and Krzeminska provided the investigators with the passwords for their devices."). Indeed, courts have even treated password protection as modestly *supporting* both the existence of "reasonable suspicion" and the reasonableness of the "scope and duration of" a border search. *See, e.g.*, *United States v. Cotterman*, 709 F.3d 952, 969-70 (9th Cir. 2013) (en banc); *Qin*, 57 F.4th at 352 (similar).

Turning away from the Fourth Amendment, Belmonte makes passing reference to a "Fifth Amendment" claim based on the "compelled provision of a passcode to an electronic device." Def. Br. 34-35 & n.18. "'A party waives an argument by failing to present it in its opening brief or by failing to develop its argument—even if its brief takes a passing shot at the issue.'" *United States v. Taylor-Sanders*, 88 F.4th 516, 525 n.5 (4th Cir. 2023). Here, Belmonte did not raise a Fifth Amendment argument before the district court, *see generally* JA25-39, JA77-89, JA103-105, and consequently failed to develop evidence that his provision of the password was involuntary, *see* JA143-170. In his opening brief on appeal, Belmonte does not even give the argument a passing shot—instead merely noting that he might have "had a Fifth Amendment right not to provide" his password, Def. Br. 34. Any such argument is therefore "waived." *Taylor-Sanders*, 88 F.4th at 525 n.5.

A Fifth Amendment argument would also fail on the merits. Among other fatal impediments, "[a]ny self-incriminating testimony that [Belmonte] may have provided by revealing the password was already a 'foregone conclusion' because the Government" could "independently prove[]" his possession of the iPhones found on him. *See, e.g.*, *United States v. Gavegnano*, 305 F. App'x 954, 956 (4th Cir. 2009) (unpublished) (per curiam); Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767, 779 (2019) ("'I know the password' is the only assertion implicit in unlocking the device.").

Independently, Belmonte could not establish his provision of the password to Officer Oliphant was involuntary. Given Belmonte's failure to develop the argument below, "the district court did not make *any* factual findings on this point" and this Court "cannot assume in the first instance that" Belmonte's unlocking of the phones was involuntary. *See Aigbekaen*, 943 F.3d at 725. For instance, Belmonte did not attempt to show that he ever read the CBP tear sheet stating that the failure to provide a device's password "may result in the detention of the device in order to complete the inspection." JA120. Instead, he left the tear sheet behind on a table and then claimed not to have received it. JA71-72. Viewed in the light most favorable to the government, Officer Oliphant's request that Belmonte provide his password was not "'coercive or threatening,'" meaning his disclosure of the

password was "voluntary" in the Fifth Amendment sense. *See, e.g.*, *United States v. Oloyede*, 933 F.3d 302, 308-09 (4th Cir. 2019).

3. Amici's novel arguments are not properly before the court and meritless.

The arguments advanced by amici—that border searches of electronic devices should require probable cause and a warrant—were not raised by Belmonte in the district court or in his "opening brief" and are therefore "waived." *United States v. Nutter*, 137 F.4th 224, 228 (4th Cir. 2025). This is Belmonte's "'case, not a joint appeal by [Belmonte] and amicus,'" meaning that he "'must raise in [his] opening brief all the issues [he] wishes the court to address." *Snyder v. Phelps*, 580 F.3d 206, 217 (4th Cir. 2009), *aff'd*, 562 U.S. 443 (2011). "Because the Court generally does not consider arguments raised in amicus . . . briefs in the first instance," it should "not reach" amici's waived "arguments here." *See, e.g.*, *M.L. by Leiman v. Smith*, 867 F.3d 487, 499 n.11 (4th Cir. 2017).

Waiver aside, amici's arguments are meritless. As one amicus concedes, Knight Br. 2 n.2, the warrant requirement advanced by the other amicus, ACLU Br. 14-19, is foreclosed by Fourth Circuit precedent. In *Nkongho*, this Court made clear that "forensic searches" and "non-routine seizures" of electronic devices at the border require only "individualized suspicion"—not a "warrant." 107 F.4th at 382-84. If non-routine border seizures and forensic searches of digital devices do not require a warrant, less intrusive manual searches certainly cannot require one.

Amici's argument that manual searches should require probable cause is no more availing. *See* Knight Br. 20-27; ACLU Br. 14-17. While this Court has technically left open the question whether *forensic* searches should require probable cause, *see, e.g.*, *Nkongho*, 107 F.4th at 382, the Supreme Court and the courts of appeals have *never* required probable cause for a border search. That is true even for highly "invasive" "strip searches, alimentary-canal searches, x-rays," *Kolsuz*, 890 F.3d at 144, and detaining a traveler "incommunicado for almost 16 hours" in a "humiliating" manner while she attempted to avoid passing drug balloons, *Montoya de Hernandez*, 473 U.S. at 542, 544. If "alimentary-canal searches" require only "reasonable suspicion," it is hard to fathom why a manual search of a cellphone would require more. *Kolsuz*, 890 F.3d at 144.

Likewise, the Knight amicus' First Amendment argument, Knight Br. 12-19, is squarely foreclosed by *Ickes*, which "h[e]ld that the border search doctrine is not subject to a First Amendment exception," 393 F.3d at 507. As with much else in this case, the other circuits to address the issue have come to the same place. *See, e.g.*, *Alasaad*, 988 F.3d at 22 ("Under any standard plaintiffs have not shown that the content-neutral border search Policies facially violate the First Amendment."); *United States v. Arnold*, 523 F.3d 941, 948 (9th Cir. 2008) (refusing "to carve out a First Amendment exception to [border search] doctrine"). As addressed above, *Ickes*' Fourth Amendment holding is fully consistent with *Riley* and *Carpenter*. *See*

supra pp. 19-22. That is all the more true of *Ickes*' First Amendment holding, about which *Riley* and *Carpenter* have absolutely nothing to say. *See generally Riley*, 573 U.S. 378 (never so much as mentioning the First Amendment); *Carpenter*, 585 U.S. 300 (same).

B. Regardless, Belmonte's suspicious payment and travel from a country known for child exploitation established reasonable suspicion to search his phones.

Reasonable suspicion requires only a "particularized and objective basis for suspecting the particular person stopped of criminal activity." *Navarette v. California*, 572 U.S. 393, 396-97 (2014). In assessing the reasonableness of the suspicion, officers may "draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that 'might well elude an untrained person.'" *United States v. Arvizu*, 534 U.S. 266, 273 (2002). "The process does not deal with hard certainties, but with probabilities." *United States v. Cortez*, 449 U.S. 411, 418 (1981). Hence, conduct that is "ambiguous and susceptible of an innocent explanation" often will support reasonable suspicion. *See Illinois v. Wardlow*, 528 U.S. 119, 125 (2000). At bottom, the reasonable suspicion standard "'is not high,'" *United States v. Grogins*, 163 F.3d 795, 797 (4th Cir. 1998), and "'falls considerably short' of 51% accuracy," *Kansas v. Glover*, 589 U.S. 376, 381 (2020).

In the context of a forensic border search, this Court has required reasonable suspicion not just of crime generally, but of "digital contraband, such as child pornography" or "evidence of ongoing transnational criminal activity, . . . such as communications between conspirators." *Nkongho*, 107 F.4th at 381.

The district court here did not err in finding that Belmonte's suspicious financial transactions with a minor suggestive of the purchase of CSAM and his travel from a country associated with child sexual exploitation established reasonable suspicion his phones contained CSAM. JA166-169.

Cash App report. Officer Oliphant knew that Cash App—a mobile payments application—had reported Belmonte (and four other users) for suspicious financial transactions with minors indicative of CSAM purchases. *See* JA149, JA155-156, JA159-160, JA163. The report covered payments from February through June 2023, approximately a year before the May 2024 search. *See* JA156-157. Further, at least one of the flagged transactions included "Snap" in the memo line. JA162-163. That was particularly significant to Officer Oliphant because she knew predators "quite frequently" "elicited" CSAM on Snapchat. JA162; *see, e.g.*, *United States v. Ninsawat*, No. 24-1276, 2025 WL 1217385, at *1 (6th Cir. Apr. 28, 2025) (unpublished) (defendant began "relationship" with "fifteen-year-old victim" on "Snapchat" and ultimately "receiv[ed] and sav[ed] at least 48 images of [the victim] engaging in sexually explicit conduct").

Belmonte's use of a mobile application to make a payment suggestive of the purchase of CSAM, and the Cash App report's reference to another mobile application (Snapchat) known for the elicitation of CSAM, thus provided Officer Oliphant ample reason to suspect Belmonte's phones might contain CSAM. *See, e.g.*, *Cotterman*, 709 F.3d at 968-69 (holding that similar "alert" flagging defendant as "'possibly involved in child sex tourism'" supported reasonable suspicion); *Touset*, 890 F.3d at 1237 (same for defendant's "three low-money transfers of $35, $35, and $37 to a Western Union account" linked to "an image of child pornography").

Belmonte suggests that the reported transactions were too stale to establish reasonable suspicion. Def. Br. 39-40. This Court, however, has recognized that issues of staleness are "different when the alleged unlawful activity involves digital images depicting child pornography . . ., in part because the nature of the property to be seized is not a consumable, like narcotics." *United States v. Ebert*, 61 F.4th 394, 401 (4th Cir. 2023). Instead, "law-enforcement experience supports the conclusion that individuals who possess such images 'rarely if ever dispose of such material, and store it for long periods in a secure place.'" *Id.* Years-old evidence of CSAM possession therefore suffices even under the more stringent "probable cause" standard. *See, e.g.*, *id.* at 398-402 ("five-to-eight-years earlier"); *United States v. Sanders*, 107 F.4th 234, 251-52 (4th Cir. 2024) ("nine-month" delay); *United States*

v. Krueger, 145 F.4th 460, 464-65 (4th Cir. 2025) ("eleven months later"). Here, the report of transactions ten-to-fifteen months before, JA156-157, falls well within the timeframe this Court has approved. Particularly so because Belmonte points to no evidence before Officer Oliphant that would have suggested he ceased purchasing CSAM or deleted the CSAM he had previously purchased. *See* Def. Br. 39-40. And furthermore, prior to this border search Belmonte had not been inspected in secondary inspection. JA70.

Shifting gears, Belmonte hypothesizes explanations for his suspicious payment to a minor. Maybe he was merely "sending lunch money to a younger sibling." Def. Br. 39. Or perhaps he purchased "marijuana," a "sexual encounter," "sexually suggestive images," or "phone sex" from a minor rather than CSAM. Def. Br. 39-40. Even assuming his scenarios do not relate to contraband or evidence of transnational crime, they fail to "construe the evidence in the light most favorable to the government," as required on appeal from the denial of a motion to suppress. *Perkins*, 363 F.3d at 320. More to the point, reasonable suspicion "'need not rule out the possibility of innocent conduct.'" *Navarette*, 572 U.S. at 403; *Perkins*, 363 F.3d at 327 (discounting "speculati[on] on possible innocent reasons for a defendant's actions"). After all, "'it must be rare indeed that an officer observes behavior consistent only with guilt and incapable of any innocent interpretation.'" *United States v. Foster*, 824 F.3d 84, 94 (4th Cir. 2016). Consequently, Belmonte's

"attempts to second-guess the officer's reasonable suspicion . . . are unavailing." *Navarette*, 572 U.S. at 403.

Nor does *Aigbekaen* undermine the district court's reasonable suspicion finding. *See* Def. Br. 41-43. There, this Court found suspicion of "domestic sex trafficking" insufficient to support a forensic border search. *See* 943 F.3d at 717-23. As a fallback argument, the government "devote[d] four sentences" to contending that the defendant's "devices 'might'" have contained "child pornography." *Id.* at 723. For sole support, the government pointed to the "brief" testimony of a police officer "that a hotel manager received a tip from an unnamed employee that the employee had 'overheard'" the defendant or his accomplice "'[saying], you know, let's hurry up and get this video done.'" *Id.* "During cross-examination," the officer admitted that the manager provided no "'indication as to why that [unnamed] employee thought that there was some type of movie making or video making going on.'" *Id.* And, critically, the "hotel manager" subsequently contradicted the officer, testifying that he did not "recall hearing *any* such statement from an employee or relating it to law enforcement." *Id.* The "isolated, vague, and third-hand allegation" there, *id.* at 724, is worlds apart from the Cash App report that Belmonte engaged in a transaction with a minor indicative of the purchase of CSAM here, *see* JA155-156.

Travel from a country known for sex trafficking. The district court did not err in finding that Belmonte's travel from Bolivia, a high-risk country for child sex

tourism and CSAM, confirmed the reasonableness of Officer Oliphant's suspicion. JA166. At the suppression hearing, Officer Oliphant explained that in her role as a Port Intelligence Officer, she reviewed information regarding CSAM "and child sex trafficking" from "CBP," "foreign and domestic law enforcement partners," and non-governmental organizations. JA145-146. As to Bolivia specifically, she had both "done research on" "trafficking trends" there and had reviewed the Bolivia section of the State Department's 2023 "Trafficking In Persons Report." JA146-147. That report showed that "they continue having issues with human trafficking" and "child sex trafficking in that country." JA147. Officer Oliphant's training and "knowledge and experience of child sex trafficking trends in Bolivia" therefore heightened her suspicion of Belmonte—who "was traveling from Bolivia via way of Colombia." JA149-150.

The district court, in turn, was permitted to "rely on" Officer Oliphant's "training and experience to support reasonable suspicion." *See United States v. Smart*, 91 F.4th 214, 225 (4th Cir. 2024). Confirming as much, courts frequently find that a defendant's travel from "from a country known for sex tourism" bolsters reasonable suspicion. *See, e.g.*, *Cotterman*, 709 F.3d at 969-69; *Touset*, 890 F.3d at 1237 (testimony "that the Philippines was a source country for child pornography"); *United States v. Wanjiku*, 919 F.3d 472, 487 (7th Cir. 2019) (defendant's return from "known destination for sex tourism").

Pushing back, Belmonte argues that Officer Oliphant's testimony is inconsistent with the State Department's Trafficking in Persons reports. Def. Br. 10-12 & nn.5-7, 40. Belmonte, however, neither introduced the reports as exhibits below nor requested the district court take judicial notice of them. Although he specifically cross-examined Officer Oliphant about the tier rankings in the 2023 report, *see* JA151-152, he never developed the record on any of the other purported inconsistencies he now raises. His attempt to undercut Officer Oliphant's testimony with new, "extra-record" material thus runs contrary to the rule that this Court is limited to the "facts" in the "record," *see, e.g.*, *United States v. Foreman*, 369 F.3d 776, 786 (4th Cir. 2004); *Aigbekaen*, 943 F.3d at 724-25 (considering only "record evidence"), which it must view in the light "most favorable" to the government, *Perkins*, 363 F.3d at 320. Moreover, even could the Court consider the extra-record material, it would be constrained to review Belmonte's arguments for plain error because he did not advance them below. *See, e.g.*, *United States v. Ojedokun*, 16 F.4th 1091, 1113 (4th Cir. 2021).

Under any standard of review, Belmonte's extra-record nitpicking fails on its own terms. He initially asserts that the report "does not have specific country-by-country information beyond identifying each country's tier." Def. Br. 10 n.5. As he belatedly concedes, Def. Br. 10 n.5, that just isn't true: the report includes country-

specific pages, including one on Bolivia. U.S. Dep't of State, *Trafficking in Persons Report: Bolivia* (2023), https://perma.cc/6HZS-MPCM.

Recognizing as much, Belmonte switches to complaining that the Bolivia section fails to address the "extent" or "rate[]" of trafficking. Def. Br. 10 n.5, 40. That too is wrong. The 2023 report, for instance, notes that Bolivian "[t]raffickers exploit an increasing number of Venezuelan victims in sex trafficking" and that "authorities reported a notable surge in the number of Venezuelan and Haitian victims of sex trafficking . . . in the country." U.S. Dep't of State, *Trafficking in Persons Report: Bolivia* (2023), https://perma.cc/6HZS-MPCM. In a related vein, Belmonte faults Officer Oliphant for not knowing the rates of sex trafficking in Virginia. Def. Br. 40. But a CBP Officer's lack of knowledge regarding domestic crime statistics does nothing to undercut the reasonableness of her suspicion regarding a traveler from a foreign country known for child sex trafficking.

Belmonte also purports that the report "treat[s] human trafficking as an 'umbrella term'" and is "not specific to child-sex offenses." Def. Br. 10 n.5. While the report addresses trafficking generally, it includes plenty of specifics on child sex trafficking. *See, e.g.*, U.S. Dep't of State, *Trafficking in Persons Report: Bolivia* (2023), https://perma.cc/6HZS-MPCM ("Child sex tourists exploited children in sex trafficking in rural Indigenous communities in the north of the La Paz department,

in and around the city of Rurrenabaque, and in tourist areas in the departments of La Paz and Beni, openly advertising to tourists speaking Hebrew and Arabic.").

Belmonte then asserts that "in the 2023 Report (the one in effect at the time of the search), Bolivia was one of 104 countries in Tier 2—along with countries like Israel, Ireland, Japan and Norway." Def. Br. 11 n.7. Wrong again. In reality, Bolivia was one of 26 countries in "Tier 2 Watch List"—along with countries like Haiti, Iraq, and Serbia. U.S. Dep't of State, *Trafficking in Persons Report* (2023), https://perma.cc/DVR8-QV2D. Tier 2 Watch List countries are those where "the estimated number of victims of severe forms of trafficking is very significant or is significantly increasing" or the country fails "to provide evidence of increasing efforts to combat severe forms of trafficking." *Id.*

Finally, Belmonte notes that the State Department's June 2024 report upgraded Bolivia from Tier 2 Watchlist to Tier 2, a category encompassing most countries. Def. Br. 40; *see* U.S. Dep't of State, *Trafficking in Persons Report: Bolivia* (2024), https://perma.cc/LSC6-DCFP. How a report issued a month "*after* the events at issue here" undercuts reasonable suspicion, Belmonte does not say. *See* Def. Br. 11 n.6, 40 (emphasis added).

All considered, the contents of the State Department report (which are not in the record) only bolster Officer Oliphant's testimony that Bolivia "continue[d] having issues with human trafficking trends, as well as child sex trafficking."

JA147. The district court therefore did not err in finding that Cash App's report of Belmonte's financial transactions with a minor suggestive of the purchase of CSAM and his travel from Bolivia sufficed for reasonable suspicion. JA166-169.

As a broader riposte, Belmonte asserts that the district court failed to apply the "reasonable suspicion standard." Def. Br. 36-39. The significance of that assertion is unclear, as this Court reviews the existence of reasonable suspicion "de novo." *Perkins*, 363 F.3d at 320. And Belmonte's claim is incorrect as well as irrelevant. He purports that the district court applied the wrong standard because it quoted *Kolsuz* for the proposition that non-routine border searches require "'some measure of individualized suspicion.'" JA166 (quoting 890 F.3d at 137). *Kolsuz* used that phrase to avoid deciding whether a forensic border search requires reasonable suspicion or probable cause, *see* 890 F.3d at 137, and there is no indication the district court applied a standard lower than reasonable suspicion here, *see, e.g.*, JA165-169. Indeed, the court expressly confirmed that it had applied the reasonable suspicion standard, emphasizing that "[e]ven if I'm wrong and the Fourth Circuit were to find that's not enough *reasonable suspicion*" the "good faith" exception would preclude suppression. JA169 (emphasis added). Belmonte ultimately appears to acknowledge as much, because he then proceeds to argue that the "district court erred by finding reasonable suspicion." Def. Br. 39.

C. At a minimum, the CBP officer acted in good faith reliance on precedent permitting manual border searches of electronic devices without reasonable suspicion.

Exclusion is a "last resort," not a "first impulse." *Herring v. United States*, 555 U.S. 135, 140 (2009) (quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006)). Even when a search is judged to be constitutionally flawed, suppression is impermissible when "'a reasonably well trained officer would'" not "'have known that'" his conduct "'was illegal.'" *United States v. Stephens*, 764 F.3d 327, 336 (4th Cir. 2014). "In such circumstances, suppression can do little to deter police misconduct, and the 'social costs' of suppression—the exclusion from trial of reliable evidence bearing on guilt or innocence—outweigh any deterrence benefits." *Kolsuz*, 890 F.3d at 147. Consequently, searches conducted "'in objectively reasonable reliance on binding appellate precedent'" are not subject to the exclusionary rule. *United States v. Hill*, 849 F.3d 195, 200 (4th Cir. 2017).

Here, Officer Oliphant acted in objectively reasonable reliance on *Ickes*' holding that manual border searches of electronic devices do not require "reasonable suspicion." 393 F.3d at 505-07. Belmonte identifies no case suggesting that officers cannot continue to rely in good faith on binding precedent merely because a subsequent decision addressing a different issue could be viewed as casting doubt on it. *See* Def. 45-46. Even to the extent this Court thought officers were obligated to pore over the pages of the United States Reports looking for cases potentially

undermining binding circuit precedent, a reasonable officer would have concluded that *Ickes* remained good law. That is so because every "'court[] of appeals to have considered the question'" after *Riley* (and *Carpenter*) affirmed *Ickes*' holding that manual border searches do not require reasonable suspicion. *United States v. Taylor*, 54 F.4th 795, 804 (4th Cir. 2022); *see supra* pp. at 21-22. Thus, even were this Court to depart from that "uniform body of" appellate "precedent," it cannot say reliance on *Ickes* was so objectively unreasonable as to preclude application of the good faith exception. *See Aigbekaen*, 943 F.3d at 725. As explained above, Belmonte also cannot escape *Ickes* by contending that this Court could have avoided deciding whether manual searches require reasonable suspicion by finding the officers had it there. *See* Def. Br. 47; *supra* pp. 22-23.

Belmonte next purports that Officer Oliphant's request for his password somehow alters the good faith analysis. Def. Br. 47. To repeat, however, the Supreme Court has made clear that border search authority extends to "locked" containers. *See, e.g.*, *Andreas*, 463 U.S. at 766-67; *supra* pp. 29-30. Consequently, no court of appeals has held that whether a phone is locked or whether the defendant reveals his password is relevant either to the substantive border search analysis or to good faith. *See supra* pp. 30-31. Given that "uniform" precedent, *Aigbekaen*, 943 F.3d at 725, Belmonte fails to proffer any reason why a reasonable officer would

"have known" the request for Belmonte's password (or the phone's encryption) precluded reliance on *Ickes*, *Stephens*, 764 F.3d at 336.

To the extent Belmonte seeks to avoid application of the good faith exception by invoking the Fifth Amendment, *see* Def. Br. 47, that argument—which was neither developed below nor squarely presented on appeal—is waived and meritless. *See supra* pp. 31-33. In brief, this Court must view the facts in the light most favorable to the government. *Perkins*, 363 F.3d at 320. And Belmonte, who did not develop the relevant facts below, came nowhere close to establishing that his knowledge of the password was not a foregone conclusion and that provision of the password was involuntary. *See supra* pp. 32-33.

Belmonte also advances a claim, likewise not raised before the district court, that the government "obfuscated" the fact that Officer Oliphant provided him a tear sheet outlining CBP's border search and asked for his password. Def. Br. 4 n.1, 47. The government, however, provided Officer Oliphant's report to defense counsel in mid-June—a month after Belmonte's arrest and two months before he filed the motion to suppress. *See* JA75-76. The report makes clear that Officer Oliphant twice gave Belmonte a CBP tear sheet (once before the search, and once afterwards when he claimed not to have previously received one) and "instructed" Belmonte to provide his password. JA71-72. In addition to being handed to Belmonte twice, the CBP tear sheet is publicly available. *See* U.S. Customs & Border Prot., *Border*

Search of Electronic Devices Tear Sheet (2023), https://perma.cc/F8DN-BNAZ. The government thus did not "obfuscate" anything. At any rate, because good faith is assessed from the perspective of an "'objectively reasonable'" officer "at the time of the search," Belmonte's dissatisfaction with the timing of discovery has no bearing on the good-faith inquiry. *Hill*, 849 F.3d at 200.

Finally, Belmonte purports that the "district court's ruling on the good-faith exception . . . should be given no deference because the court applied the wrong legal standard." Def. Br. 47. But the district court specifically referenced "*Kolsuz*" (where this Court found good faith, 890 F.3d at 148) and analogized to the circumstances there. JA169. Further, "whether the exclusionary rule renders the evidence inadmissible" is a "legal conclusion" this Court reviews "de novo." *Stephens*, 764 F.3d at 334-35. So, it is unclear what "deference" Belmonte seeks to avoid. Def. Br. 47.

Conclusion

This Court should affirm the judgment of the district court.

Respectfully submitted,

Lindsey Halligan
United States Attorney
Special Attorney

Todd W. Blanche
Deputy Attorney General

Robert K. McBride
First Assistant United States Attorney

/s/
Lauren Halper
Assistant United States Attorneys

Statement Regarding Oral Argument

The United States respectfully suggests that oral argument is not necessary in this case. The legal issues are not novel, and oral argument likely would not aid the Court in reaching its decision.

Certificate of Compliance

I certify that this brief was written using 14-point Times New Roman typeface and Microsoft Word 365.

I further certify that this brief does not exceed 13,000 words (and is specifically 11,301 words) as counted by Microsoft Word, excluding the table of contents, table of authorities, statement regarding oral argument, this certificate, the certificate of service, and any addendum.

I understand that a material misrepresentation can result in the Court's striking the brief and imposing sanctions.

/s/
Lauren Halper
Assistant United States Attorney