No. 25-4239

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
***Plaintiff/Appellee*,**

v.

JOSE BELMONTE CARDOZO,
Defendant/Appellant.

On Appeal From the United States District Court
for the Eastern District of Virginia
Alexandria Division (The Hon. Leonie M. Brinkema)

BRIEF OF THE APPELLANT

GEREMY C. KAMENS
Federal Public Defender

Todd M. Richman
Salvatore M. Mancina
Assistant Federal Public Defenders
Counsel for Appellant
1650 King Street, Suite 500
Alexandria, VA 22314
(703) 600-0800
Todd_Richman@fd.org
Sam_Mancina@fd.org

TABLE OF CONTENTS

Table of Authorities iii

Statement of Jurisdiction 1

Statement of the Issues 2

Statement of the Case 2

A. The Search of Mr. Belmonte Cardozo's Phone upon His Arrival at Dulles Airport 2

B. Mr. Belmonte Cardozo's Motion to Suppress 6

C. The Hearing on the Motion to Suppress 9

D. Mr. Belmonte Cardozo's Entry of a Conditional Plea 16

Summary of Argument 17

Standard of Review 19

Argument 20

I. The District Court Correctly Required An Individualized Showing Of Reasonable Suspicion To Search A Cell Phone At The Border. 20

A. Exceptions to the Warrant Requirement Are Narrowly Construed, and Their Scope Is Limited by the Justification Allowing an Exception. 20

B. Following the Supreme Court's Admonition That Cell Phones Raise Unique Privacy Concerns, This Court Has Required Individualized Suspicion for Limited Forensic Searches of Cell Phones at the Border. 22

C. While This Court Has Not Addressed Manual Phone Searches at the Border, the Manual/Forensic Distinction Should Not Matter Because a Manual Search is Just as Privacy-Intrusive as a Forensic Search. 25

D. The Extraordinary Privacy Interests at Stake in Searching Modern Smartphones Are Too Great to Leave to Law Enforcement Officers' Unreviewable Discretion.....32

II. The Search Of Mr. Belmonte Cardozo's Smart-Phones Was Not Supported By Reasonable Suspicion.....35

A. The District Court Erred by Not Applying the Reasonable Suspicion Standard or Requiring a Nexus to an Ongoing Transnational Offense. 36

B. The District Court Erred by Finding Reasonable Suspicion on the Basis of Vanishingly Thin Evidence.....39

III. The Good-Faith Exception Does Not Apply Because No Binding Precedent Authorizes Suspicionless Phone Searches Or Allows Law Enforcement To Require Travelers To Provide Their Passcodes. 44

Conclusion 48

Request For Oral Argument.....50

Certificate of Compliance

TABLE OF AUTHORITIES

Cases

Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir. 2021) 31

Arizona v. Gant, 556 U.S. 332 (2009) 21, 22

Carpenter v. United States, 585 U.S. 296 (2018) 23, 24

Chimel v. California, 395 U.S. 752 (1969) 21

Coolidge v. New Hampshire, 403 U.S. 443 (1971) 21

Davis v. United States, 564 U.S. 229 (2011) 44

Illinois v. Wardlow, 528 U.S. 119 (2000) 44

In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012) 34

Katz v. United States, 389 U.S. 347 (1967) 21

New York v. Belton, 453 U.S. 454 (1981) 21

Riley v. California, 573 U.S. 373 (2014) ..... *passim*

Taylor v. Alabama, 457 U.S. 687 (1982) 20

Terry v. Ohio, 392 U.S. 1 (1968) 38

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

United States v. Alisigwe, No. 22-cr-425, 2023 WL 8275923 (S.D.N.Y. Nov. 30, 2023) 28

United States v. Apple MacPro Computer, 851 F.3d 238 (3d Cir. 2017) 35

United States v. Arvizu, 534 U.S. 266 (2002) 38

United States v. Baker, 719 F.3d 313 (4th Cir. 2013) 44

United States v. Black, 707 F.3d 531 (4th Cir. 2013) 38

United States v. Brown, 125 F.4th 1186 (D.C. Cir. 2025) 34

United States v. Brown, 401 F.3d 588 (4th Cir. 2005) 20

United States v. Bundy, 392 F.3d 641 (4th Cir. 2004) 17

United States v. Buster, 26 F.4th 627 (4th Cir. 2022) 20

United States v. Cano, 934 F.3d 1002 (9th Cir. 2019) 31

United States v. Castillo, 70 F.4th 894 (5th Cir. 2023) 31

United States v. Chadwick, 433 U.S. 1 (1977) 23

United States v. Cortez, 449 U.S. 411 (1981) 38

United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (*en banc*) 31

United States v. Davis, 690 F.3d 226 (4th Cir. 2012) 20

United States v. Feliciana, 974 F.3d 519 (2020) 39, 41

United States v. Foster, 634 F.3d 243 (4th Cir. 2011) 38

United States v. Gavino, No. 22-cr-136, 2024 WL 85072 (E.D.N.Y. Jan. 7, 2024) 28

United States v. Ickes, 393 F.3d 501 (4th Cir. 2005) 9, 46, 47

United States v. Jenkins, 850 F.3d 912 (7th Cir. 2017) 44

United States v. Kolsuz, 185 F. Supp. 3d 843 (E.D. Va. 2016) 18

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

United States v. Massenburg, 654 F.3d 480 (4th Cir. 2011) 38, 44

United States v. McCoy, 513 F.3d 405 (4th Cir. 2008) 39

United States v. Mendez, 103 F.4th 1303 (7th Cir. 2024) 31

United States v. Montoya de Hernandez, 473 U.S. 531 (1985).....17

United States v. Peters, 60 F.4th 855 (4th Cir. 2023).....44

United States v. Ramsey, 431 U.S. 606 (1977).....17

United States v. Robinson, 414 U.S. 218 (1973).....23

United States v. Robinson, No. 23-cr-192, 2025 WL 1359352 (E.D.N.Y. May 9, 2025).....28

United States v. Saboonchi, 990 F. Supp. 2d 536 (D. Md. 2014).....26

United States v. Smith, 673 F. Supp. 3d 381 (S.D.N.Y. 2023).....31

United States v. Sultanov, 742 F. Supp. 3d 258 (E.D.N.Y. 2024)..... 28, 29, 32

United States v. Touset, 890 F.3d 1227 (11th Cir. 2018).....30

Wong Sun v. United States, 371 U.S. 471 (1963).....20

Constitutional Provisions, Statutes, and Rules

U.S. Const. amend. IV ..... *passim*

18 U.S.C. § 2251.....16

18 U.S.C. § 2252.....16

18 U.S.C. § 2422.....16

18 U.S.C. § 3231.....1

28 U.S.C. § 1291.....1

Fed. R. App. P. 4.....1

Fed. R. Crim. P. 11.....16

Other Authorities

2024 Trafficking in Persons Report: Bolivia, U.S. DEP'T OF STATE, https://tinyurl.com/ycy8huw9 (last accessed October 21, 2025).....10

Border Search of Electronic Devices at Ports of Entry, U.S. CUSTOMS AND BORDER PROT., https://tinyurl.com/3cu27jm9 (last accessed October 19, 2025) 32, 33

CBP Directive No. 3340-049A § 5.4.1.2 (Jan. 4, 2018), available at https://tinyurl.com/bdz88dzb 27

CBP Statement on Border Searches of Electronic Devices, U.S. CUSTOMS AND BORDER PROT. (Oct. 30, 2019), https://tinyurl.com/2ekpcrc9.....32

Cong. Rsch. Serv., R4407.5, *Encryption: Selected Legal Issues* (2016), available at https://tinyurl.com/4bnv8bec.....7

Cracks in the Wall: When Border Watchdogs Turn Criminal, TEXAS TRIBUNE (July 7, 2016), https://tinyurl.com/mskbsfjv.....34

Customs and Border Protection Officer Arrested for Receiving Sexual Favors in Exchange for Allowing Aliens to be Smuggled Through His Lane, FBI SAN DIEGO (Sep. 8, 2016), https://tinyurl.com/2mwk8h43 34

David E. Sanger and Brian X. Chen, *Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.*, N.Y. TIMES (Sept. 26, 2014), https://tinyurl.com/y99rkwv2.....7

Encryption Technology and Potential U.S. Policy Responses: Hearing Before Subcomm. on Info. Tech. of the H. Comm. On Oversight and Gov't Reform, 114th Cong. 5–6 (2015) (statement of Amy Hess, Exec. Asst. Director, Science and Tech. Branch, FBI), available at https://tinyurl.com/2jbnfr5d.....7

Eric G. Benotsch et al., *Sexting, Substance Use, and Sexual Risk Behavior in Young Adults*, 52 J. ADOLESC. HEALTH 307 (2013).....5

Farhad Manjoo, *Taking a Naked Selfie? Your Phone Should Step in to Protect You*, N.Y. TIMES (Sept. 5, 2014), https://tinyurl.com/yc3t6rhv.....5

How to Protect the Data That is Stored on Your Devices, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, https://tinyurl.com/m24rkpu3 (last accessed Oct. 19, 2025) 7

iPhone User Guide: Search for Photos and Videos on iPhone, APPLE, https://tinyurl.com/28bys7x6 (last accessed Oct. 15, 2025) 26

iPhone User Guide: Set a Passcode on iPhone, APPLE, https://tinyurl.com/2bmp5cww (last accessed Oct. 19, 2025) 7

Julia Ainsley, *A Top Border Patrol Official Resigned After Allegedly Pressuring Female Employees for Sex, Officials Say*, NBC NEWS (Jan. 21, 2023), https://tinyurl.com/4jv4jndm 34

Justin Doubleday, *DHS prepares for unprecedented spending surge under 'Big, Beautiful Bill'*, FEDERAL NEWS NETWORK (July 7, 2025), https://tinyurl.com/22mt3rnx 33

Kerr, *Foreword: Accounting for Technological Change*, 36 Harv. J.L. & Pub. Pol'y 403 (2013) 23

Margy O'Herron, *Big Budget Act Creates "Deportation-Industrial Complex"*, BRENNAN CENTER FOR JUSTICE (Aug. 13, 2025), https://tinyurl.com/ycxf6ekd 33

Sheri Madigan et al., *Prevalence of Multiple Forms of Sexting Behavior Among Youth, A Systemic Review and Meta-analysis,* 172 JAMA PEDIATRICS 327 (2018) 5

Trafficking in Persons Report, U.S. DEP'T OF STATE, https://tinyurl.com/mt46m3b9 (last accessed Oct. 21, 2025) 11

U.S. DEP'T OF STATE, 2023 TRAFFICKING IN PERSONS REPORT (June 2023), available at https://tinyurl.com/yc5fsz4m 10, 11, 40

U.S. DEP'T OF STATE, 2024 TRAFFICKING IN PERSONS REPORT (June 2024), available at https://tinyurl.com/4ea932en 12

U.S. SENT'G COMM'N, *Quarterly Data Report, Fiscal Year 2024* (2024), https://tinyurl.com/4zkvkfhw 33

United States v. Aigbekaen, Supp. Br. of the Appellee, 2019 WL 268482 (Jan. 17, 2019) 42

No. 25-4239

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH COURT

UNITED STATES OF AMERICA,
Plaintiff/Appellee,

v.

JOSE BELMONTE CARDOZO,
Defendant/Appellant.

On Appeal From the United States District Court
for the Eastern District of Virginia
Alexandria Division (The Hon. Leonie M. Brinkema)

BRIEF OF THE APPELLANT

STATEMENT OF JURISDICTION

The district court had jurisdiction over this federal criminal case pursuant to 18 U.S.C. § 3231. That court entered the order of judgment and conviction on April 15, 2025. J.A. 240. Mr. Belmonte Cardozo filed his notice of appeal on April 29, 2025. J.A. 249; *see* Fed. R. App. P. 4(b)(1), (b)(6). Therefore, this Court has jurisdiction over this appeal pursuant to 28 U.S.C. § 1291.

STATEMENT OF THE ISSUES

I. In *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018), this Court held that individualized suspicion of an ongoing transnational offense is required to permit a limited forensic search of a non-password-protected cell phone at the border. Is the same level of suspicion required to manually search a password-protected cell phone at the border where the manual search accesses all the same information and where customs agents access the most private files on the phone?

II. Did the district court err in finding individualized reasonable suspicion where the only individualized evidence was that Mr. Belmonte Cardozo had traveled internationally on one occasion and had made at least one payment to a minor, for an unknown reason, between ten and fifteen months prior to the search?

III. Did the district court err in finding good-faith reliance on binding precedent where neither the Supreme Court nor this Court has ruled that federal agents may, without any individualized suspicion, manually search the contents of a smartphone during a border crossing or demand the passcode to unlock it?

STATEMENT OF THE CASE

A. The Search of Mr. Belmonte Cardozo's Phone upon His Arrival at Dulles Airport

On May 8, 2024, Mr. Belmonte Cardozo, a United States citizen returning from a family visit to Bolivia, arrived at Dulles Airport on a flight from Bogota, Colombia, that had originated in Santa Cruz, Bolivia. J.A. 25, J.A. 41. While going

through customs, Mr. Belmonte Cardozo was referred by Customs and Border Protection ("CBP") agents to "secondary inspection." J.A. 41. At secondary inspection, he was met by CBP Port Intelligence Officer Sara Oliphant, who had placed a "lookout" for Mr. Belmonte Cardozo in a CBP database, instructing CBP officers to refer him to secondary inspection upon arrival. J.A. 41.

Once Mr. Belmonte Cardozo arrived at the secondary inspection area, Officer Oliphant escorted him to retrieve his baggage and then brought him back to secondary inspection. J.A. 41. She and her partner first did a "full bag exam," which she described as a traditional search of a traveler's physical belongings. J.A. 160. She determined that he had two Apple iPhones in his possession, which were locked. J.A. 41–42. Mr. Belmonte Cardozo was "instructed" to provide the passcode to unlock his devices. J.A. 71. Officer Oliphant also gave him a CBP "tear sheet which outlines [CBP's] border search authority of electronics and asked for his devices." JA. 160–161.

The CBP "tear sheet" informed Mr. Belmonte Cardozo that he was "obligated to present electronic devices and the information resident on the device in a condition that allows for the examination of the device and its contents." J.A. 120; *see also* J.A. 104 (government stipulation that the "tear sheet" identified by defense counsel (J.A. 120–121) is an authentic copy of the form that had been provided to Mr.

Belmonte Cardozo, although it was not produced in discovery).[1] Mr. Belmonte Cardozo, as instructed, unlocked his devices, and Officer Oliphant "wrote the passcode down" in case she needed it again. J.A. 161.

Officer Oliphant explained that, because she was conducting an exam for child pornography, "I know based on my experience that a lot of times this can be hidden in hidden apps, … [or] in the hidden gallery of the iPhone's photo gallery. So that is the first place that I … look." J.A. 161. As a defense forensic expert later explained,

> [Hidden] folders are typically used for a person's most private information—for example, hidden folders can be used to keep backup copies of important documents in the event that one loses one's wallet or identification. By placing into a hidden folder photos that a person wishes to store in a secure place (for example, photos of the user's driver's license, passport, credit cards or other private items that they wish to have available but not readily accessible to others), the user can keep those materials accessible while also making them invisible to anyone but the owner. For example, if one allows a friend to look through a photo album by handing that person one's

[1] In proceedings below, the government repeatedly elided the fact that CBP had ordered Mr. Belmonte Cardozo to provide his passcode. Instead, the government falsely informed the court on two occasions—once under oath—that Mr. Belmonte Cardozo had "voluntarily" provided his passcode to CBP. *See* J.A. 14, J.A. 42. A law-enforcement report, however, mentioned that he had been "instructed" to provide his passcode, and cryptically referred to him receiving a "BSED tear sheet." *See* J.A. 71. It was only after defense counsel identified a copy of the CBP "tear sheet" titled "Border Search of Electronic Devices" (which states that travelers are "obligated" to unlock their devices (*see* J.A. 120-121)) that the government disclaimed any reliance on consent and acknowledged that CBP had ordered Mr. Belmonte Cardozo to unlock his devices. J.A. 103-104.

> unlocked iPhone, the recipient will be able to review the owner's other photos, but will not see photos that had been placed in a hidden folder. Moreover, such a person would not be able to open the hidden folder unless the owner had provided the passcode to that person.

J.A. 110.[2]

Approximately two minutes into her search, Officer Oliphant found an image that she believed to be child pornography. J.A. 162. Within about ten minutes after commencing her search of the phone, Officer Oliphant notified Homeland Security Investigations ("HSI"). J.A. 43. She then continued her search of the phone, looking for "disguising applications" or "a hidden storage vault" (neither of which existed), and reviewed Mr. Belmonte Cardozo's social media applications. J.A. 43. HSI agents responded, and undertook a further examination of the phones, which lasted about one hour. J.A. 43. After detaining the phones based on those initial findings,

[2] Another example of items that might commonly be placed in "hidden" folders would be consensually taken nude photos of oneself or an intimate partner. *See* Eric G. Benotsch et al., *Sexting, Substance Use, and Sexual Risk Behavior in Young Adults*, 52 J. ADOLESC. HEALTH 307, 308 (2013) (finding that "19% of teenagers (ages 13–19) and 32% of young adults (ages 20–26) reported sending a nude or semi-nude picture or video of themselves to someone via text or e-mail"); Sheri Madigan et al., *Prevalence of Multiple Forms of Sexting Behavior Among Youth, A Systemic Review and Meta-analysis,* 172 JAMA PEDIATRICS 327, 328 (2018) (among 39 included studies, 14.8% of 15-16 year-olds had sent "sexts," and prevalence increased with age); Farhad Manjoo, *Taking a Naked Selfie? Your Phone Should Step in to Protect You*, N.Y. TIMES (Sept. 5, 2014), https://tinyurl.com/yc3t6rhv ("Surveys suggest that by the time they finish college, a third of young people have snapped and sent naked photos of themselves to others.").

HSI "conducted a forensic border search of the iPhones." J.A. 44–45. That same evening, while still in customs at Dulles Airport, Mr. Belmonte Cardozo was arrested and taken into HSI custody. JA. 44.

B. Mr. Belmonte Cardozo's Motion to Suppress

Mr. Belmonte Cardozo moved to suppress, arguing that the search of his phones exceeded the scope of a routine border search for several reasons. First, while the initial search was conducted manually rather than using forensic software, it exposed all the same information that had been reviewed in *Kolsuz*, where this Court found that a forensic search was non-routine because of its extensive scope and intrusiveness. *See* J.A. 36. Second, an iPhone's onboard operating system allows for efficient searching of a phone's contents in ways that are often more efficient than forensic software, blurring the lines between forensic and non-forensic searches. *See* J.A. 36, J.A. 81–82. Third, Officer Oliphant immediately accessed the most private files on the phone—those that had been "hidden" and would not have been seen even by a friend of the owner who was given the phone to scroll through its contents. *See* J.A. 36, J.A. 82–83. And fourth, the phone was passcode-protected and unlocked only because CBP ordered Mr. Belmonte Cardozo to unlock it. J.A. 28, J.A. 35–36. Indeed, but for the CBP's directive to unlock the phone, the only means of searching it without the passcode would have been a forensic search, which would have required individualized suspicion under *Kolsuz*. *See* J.A. 123–

124 (notice of testimony of government forensic examiner that forensic software could have extracted most of the phone's contents had CBP received the phone without the passcode).[3]

[3] iPhones have been encrypted by default since 2014—meaning that they are encrypted by the act of establishing a passcode and decrypted each time the passcode is entered. *See iPhone User Guide: Set a Passcode on iPhone*, APPLE, https://tinyurl.com/2bmp5cww (last accessed October 19, 2025) ("set[ting] a passcode … to unlock iPhone when you turn it on or wake it … turns on data protection, which encrypts your iPhone"); David E. Sanger and Brian X. Chen, *Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.*, N.Y. TIMES (Sept. 26, 2014), https://tinyurl.com/y99rkwv2 (reporting that the iPhone 6 was the first phone to "encrypt[] emails, photos and contacts based on a complex mathematical algorithm"); *Encryption Technology and Potential U.S. Policy Responses: Hearing Before Subcomm. on Info. Tech. of the H. Comm. On Oversight and Gov't Reform*, 114th Cong. 5–6 (2015) (statement of Amy Hess, Exec. Asst. Director, Science and Tech. Branch, FBI), available at https://tinyurl.com/2jbnfr5d ("[W]ith today's new operating systems, a device and all of a user's information on that device can be encrypted by default"); Cong. Rsch. Serv., R4407.5, *Encryption: Selected Legal Issues* 1 (2016), available at https://tinyurl.com/4bnv8bec ("In 2014, three of the biggest technology companies in the United States—Apple, Google, and Facebook—began encrypting their devices and communication platforms by default."); *How to Protect the Data That is Stored on Your Devices*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, https://tinyurl.com/m24rkpu3 (last accessed Oct. 19, 2025) (to set up system encryption on an iPhone, set a passcode).

While the government's forensic examiner contends that forensic software could have extracted most of the phone's contents even without the passcode, that is not because it was unencrypted. Rather, once an iPhone has been unlocked for the first time after powering on, the decryption key is moved from the system's Secure Enclave into memory for easy decryption each time the passcode is entered—and the forensic software can retrieve it from the phone's memory. *See Understanding AFU vs BFU in iPhone Forensics and Encryption*, SALVATION DATA TECH. (May 12, 2025), https://tinyurl.com/28fzezz5.

Accordingly, Mr. Belmonte Cardozo argued that the search had to be treated as a non-routine border search, which requires an individualized showing of reasonable articulable suspicion, *see* JA 35–36, or alternatively as a non-border search predicated on the government's "generalized interest in law enforcement and combatting crime" (which would require a warrant supported by probable cause). J.A. 36 (quoting *Kolsuz*, 890 F.3d at 143). Because the government had refused to produce discovery about CBP's basis for the original "lookout"—believing, incorrectly, that *Kolsuz* had held that manual searches required no individualized suspicion, *see* JA 75–76[4]—Mr. Belmonte Cardozo argued that the fruits of the search should be suppressed in the absence of any such evidence. JA 37.

The government opposed the motion to suppress, arguing that no individualized suspicion was necessary based largely on the fact that the search was "manual" and led quickly to the identification of apparent images of child pornography. JA 54–61. Further, the government argued that if reasonable suspicion were necessary, it existed in this case because of the facts underlying the "lookout" (an issue on which the government had by then produced discovery)—specifically, the fact that Mr. Belmonte Cardozo was traveling from Bolivia, a "high-risk country for child sex tourism and child sexual exploitation material," and the

[4] In fact, *Kolsuz* expressly stated that it did not address the level of suspicion required for manual searches. *See Kolsuz*, 890 F.3d at 140 n.2, 141.

fact that he had engaged in "potentially suspicious financial transactions." JA. 62. Finally, the government argued that even if reasonable suspicion were determined to have been necessary and not to exist, suppression should be denied because the officers were acting in good faith reliance on binding precedent. By this time, the government had abandoned its earlier contention that *Kolsuz* expressly permitted manual searches of smartphones at the border without suspicion, *see* J.A. 75, but instead relied upon a case that never mentioned smartphones and was decided two years before the first iPhone was released, *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005). J.A. 63–66.

C. The Hearing on the Motion to Suppress

After thorough briefing on the Motion, including submissions by both parties on the relevant digital forensic issues, the district court held a motion hearing at which it instructed the parties to move directly to the issue of reasonable suspicion. *See* J.A. 143–144 (instructing the government to call Officer Oliphant and noting that it would not need forensic testimony).

On direct examination, Officer Oliphant first reviewed her experience as a CBP agent and Port Intelligence Officer, a position she had held for less than a year at the time of the search. J.A. 145–156. Next, she testified to the three pieces of evidence that caused her to place a lookout for Mr. Belmonte Cardozo. First, she referred to the State Department's Trafficking in Persons Report. J.A. 146–147. She

testified she had reviewed the Report "specific to Bolivia, which I've done research on. And it just shows that they continue having issues with human trafficking trends, as well as child sex trafficking in that country." J.A. 147. She further explained that "[w]hen you review the report, you can go in country by country and read up specifically on whatever you're looking for country-wise." *Id.*[5] Second, Officer Oliphant testified that Mr. Belmonte Cardozo was listed in a report from the CBP National Targeting Center "of names that have been gathered … of travelers that have potentially suspicious financial data that would be indicative of possible CSAM

[5] This is not true. The Trafficking in Persons Report divides countries into three tiers and does not have specific country-by-country information beyond identifying each country's tier. Neither the 2023 nor the 2024 Trafficking in Persons Reports has any such country-by-country information. The word "Bolivia" is mentioned in the 2023 Report, for example, only in the tier listings and in a brief profile of a person who was forced to traffic drugs between Bolivia and Chile. *See* U.S. DEP'T OF STATE, 2023 TRAFFICKING IN PERSONS REPORT 26, 86 (June 2023), available at https://tinyurl.com/yc5fsz4m. The State Department's website does allow users to sort country-by-country, but the country-specific webpages merely describe that country's anti-trafficking practices (not each country's trafficking rates). *See 2024 Trafficking in Persons Report: Bolivia*, U.S. DEP'T OF STATE, https://tinyurl.com/ycy8huw9 (last accessed October 21, 2025).

Indeed, neither the reports nor the country-specific webpages focus on the *extent* of trafficking activities in each country. Rather, they grade each country based on its efforts to combat trafficking. *See* 2023 TRAFFICKING IN PERSONS REPORT, *supra*, at 70 (tier "placement is based not on the size of a country's problem but on the extent of government efforts to meet the [Trafficking Victims Protection Act's] minimum standards for elimination of human trafficking"). Moreover, the reports are not specific to child-sex offenses; rather, they treat human trafficking as an "umbrella term" that includes forced labor, adult sex trafficking and child sex trafficking. *Id.* at 39–42.

[child sexual abuse material] purchases." J.A. 147–149. Third, Officer Oliphant testified that CBP was running "a special operation" in May 2024, focusing on CSAM. J.A. 148. In sum, the lookout for Mr. Belmonte Cardozo was premised on (i) the State Department Report (combined with travel to Bolivia), (ii) the financial transactions, and (iii) "[CBP's] operation" to focus on CSAM. J.A. 150.

Officer Oliphant did not identify any additional evidence that arose during her interactions with Mr. Belmonte Cardozo, such as nervousness or evasiveness. Accordingly, the three bases for the lookout also formed the totality of any suspicion she had to search his electronic devices.

On cross-examination, Officer Oliphant did not dispute that Bolivia was in Tier 2 of the State Department Trafficking in Persons Report for 2024. J.A. 152.[6] Further, when asked whether she agreed that the "vast majority" of countries in the world were within Tier 2, she responded "perhaps," J.A. 152.[7] Although she claimed

[6] This was true with respect to the 2024 report, which was issued in June 2024 (shortly after the events at issue here), and with respect to the 2023 report. *See Trafficking in Persons Report*, U.S. DEP'T OF STATE, https://tinyurl.com/mt46m3b9 (last accessed Oct. 21, 2025).

[7] They are. 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. There were only 30 countries in Tier 1 (each of which had demonstrated best practices with respect to human trafficking), and 24 in Tier 3 (each of which had the most concerning practices with respect to human trafficking). *See* 2023 TRAFFICKING IN PERSONS REPORT, *supra* note 5, at 86. The 2024 Report is similar and also places Bolivia in Tier 2 with the great majority of countries. *See*

to have "done research on" human trafficking in Bolivia, J.A. 147, she could not answer whether the suspicion regarding a person arriving from Bolivia would extend only to citizens of Bolivia, or to anyone transiting through or visiting Bolivia. J.A. 153 (answering "I suppose. It would depend on the verbiage of the report.")

Officer Oliphant followed her non-answer to that question by moving on to a claim that Bolivia had "increased rates of child sex trafficking, and I believe sex child tourism as well." J.A. 153–154. But she could not explain what she meant by that:

> Q. Increased compared to what?
>
> A. General trends, as far as I'm aware.
>
> Q. Higher than, say, Virginia?
>
> A. I'm unaware of that.
>
> ….
>
> Q. So you don't know if Bolivia has a higher rate of CSAM trafficking or child sex trafficking than Virginia?
>
> A. I'm unaware.
>
> Q. So you don't know if people coming from Bolivia have any higher risk than every single person landing at Dulles; right?
>
> A. I'm unaware.

U.S. DEP'T OF STATE, 2024 TRAFFICKING IN PERSONS REPORT 65 (June 2024), available at https://tinyurl.com/4ea932en.

J.A. 154.

Officer Oliphant's testimony about the "potentially suspicious financial data" was that CBP had received a report from another government agency, FINCEN, which was passing along information it had received from a private party that operated a payment app. J.A. 155. Further, she testified that Mr. Belmonte Cardozo's name was included in that report among "a list of people that the company had identified as sending money to accounts associated with minors." J.A. 155. The report did not show whether the listed people "could even see whether the accounts were associated with minors." J.A. 155. Further, she testified that the payment company—which is not itself a place where people can transfer images—would not have any way of knowing what the payments were for, other than whatever insight could be gleaned from the memo lines associated with each payment. J.A. 155–156. Nor did the report identify any witness who said that any of the payments were related to CSAM. J.A. 156.

According to Officer Oliphant, the memo lines—some of which said things like "food and stuff"—were the basis for Mr. Belmonte Cardozo, and several other people, being reported to FINCEN. J.A. 156.[8] She did not claim to know the content

[8] Later, Officer Oliphant explained that "one" of the memo lines listed in the report from the private company to FINCEN used the word "Snap," which she found suspicious because it appeared to be a reference to Snapchat—an app that, among other uses, can be used to trade CSAM. J.A. 162. She did not know, however,

of any memo line attributed to Mr. Belmonte Cardozo. J.A. 156. Nor did she know whether the inclusion of Mr. Belmonte Cardozo in the report was based on multiple transactions or only "a particular charge." J.A. 156–157. Further, because the report was related to transactions over a five-month period beginning in February of 2023, she agreed that his inclusion in the report could have been based on a single financial transaction that occurred somewhere between ten to fifteen months before the search of Mr. Belmonte Cardozo's electronic devices at Dulles. J.A. 157–158.

When asked whether she had any knowledge of "anything [that] was ongoing as of May 2024," she testified that she had none. J.A. 158. In fact, she did not even know whether the transactions were ongoing throughout the five-month period in 2023 covered by the report. J.A. 157 ("I'm unaware if it was ongoing or if it was a particular charge"). Finally, when asked whether the report gave any information to show that any of the transactions were transnational, Officer Oliphant testified "I don't believe so." J.A. 158.

With respect to the third category of information Officer Oliphant identified as supporting her suspicion about Mr. Belmonte Cardozo—the fact that CBP was running an operation that month focused on interdicting CSAM—she did not testify

---

whether that single reference to "Snap" had anything to do with Mr. Belmonte Cardozo. J.A. 163.

how the fact of that operation in any way contributed to individualized suspicion regarding Mr. Belmonte Cardozo.

After hearing Officer Oliphant's testimony, the district court denied the motion to suppress. The court found that "Officer Oliphant did have some measure of individualized suspicion." J.A. 166. In the court's view, "she clearly knew, Number 1, that the defendant was coming from a country that does have some connection with child sex trafficking and child sex tourism." J.A. 166. While "that fact alone would not have been enough," the court found, she also knew of "defendant's name appearing on a particular alert, which is apparently a standard type of alert system for law enforcement." J.A. 166. Finally, the court also noted that "the customs folks had decided to make May a particular month" focused on CSAM interdiction and found that "these three factors" combined to "establish that there was some individualized suspicion as to this defendant." J.A. 167.

Further, the district court held 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 save this search because "everything that I see here is good law enforcement practice." J.A. 169. The court followed its oral ruling with a written Order denying the motion to suppress, which did not provide any further reasoning. J.A. 171.

D. Mr. Belmonte Cardozo's Entry of a Conditional Plea

Following his arrest at Dulles Airport, Mr. Belmonte was charged by Criminal Complaint with Transportation of Child Pornography in violation of 18 U.S.C. § 2252(a)(1) and (b)(1). J.A. 10. He was later indicted on that charge, J.A. 18–19, and additional charges were added in a Superseding Indictment, J.A. 20–24, and then in a Second Superseding Indictment. J.A. 90–102.

Following the denial of his Motion to Suppress, Mr. Belmonte pleaded guilty to all ten counts in the Superseding Indictment: five counts of sexual exploitation of a minor under 18 U.S.C. § 2251(a) and (e) (for inducing minors to create visual depictions of sexually explicit conduct); two counts of coercion and enticement of a minor to engage in illegal sexual activity in violation of 18 U.S.C. § 2422(b) (for causing minors to distribute images of child pornography to him); and one count each of transportation, receipt and possession of child pornography in violation of 18 U.S.C. § 2252(a)(1), (a)(2), (a)(4)(B), (b)(1) and (b)(2). *See* J.A. 209–226 (Plea Agreement); JA. 172–208 (Trans. of Plea Hearing).

The Plea Agreement was conditional pursuant to Fed. R. Crim. P. 11(a)(2). Specifically, the agreement preserved Mr. Belmonte Cardozo's right to appeal the district court's denial of his motion to suppress. J.A. 217. The district court orally reviewed the conditional language of the Plea Agreement at the plea hearing and accepted the plea. J.A. 191, J.A. 205. Further, because all evidence underlying all

ten counts of the Superseding Indictment are fruits of the challenged search of Mr. Belmonte Cardozo's iPhones, the issue preserved for appeal is case-dispositive. *See United States v. Bundy*, 392 F.3d 641, 647–49 (4th Cir. 2004).

SUMMARY OF ARGUMENT

I. The iPhone search in this case required individualized reasonable suspicion. The border-search exception to the Fourth Amendment's warrant requirement is premised on "the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country." *United States v. Ramsey*, 431 U.S. 606, 620 (1977). The exception permits customs agents to engage only in "routine" searches "without a warrant or any individualized suspicion." *United States v. Kolsuz*, 890 F.3d 133, 137 (4th Cir. 2018). Where such a search is particularly intrusive, however, it becomes "nonroutine" and must be supported by individualized reasonable suspicion. *Id*. at 138 (citing *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985)). Further, to assure that searches under the border-search exception are sufficiently tethered to the justification permitting a warrant exception, the reasonable individualized suspicion in such a case must relate to an "ongoing transnational crime." *Id*. at 143–44.[9]

[9] Where a search occurs during a border crossing but is conducted to further the government's "generalized interest in law enforcement and combatting crime," "the government interests underlying a Fourth Amendment exception are not

Considering the extraordinary privacy implications surrounding searches of modern smartphones, this Court found in *Kolsuz* that a limited forensic search of a non-password-protected smartphone at the border—or at its functional equivalent, such as an international airport—is a "nonroutine" search that must be based on at least individualized reasonable suspicion of an ongoing transnational offense. *Id*. at 144–46, 148.

As in *Kolsuz*, the search here should be deemed nonroutine. While it was "manual" rather than forensic, the search in this case implicated every type of private information that was at issue in *Kolsuz*, which involved a limited forensic search of those parts of the device visible to an ordinary user. *Id*. at 145 n.4; *see also United States v. Kolsuz*, 185 F. Supp. 3d 843, 849 & n.8 (E.D. Va. 2016) (explaining that the *Kolsuz* search included only those files that would be "easily accessible" on the device). Moreover, the device in *Kolsuz*, unlike Mr. Belmonte Cardozo's device, was non-password-protected. 890 F.3d at 139. And the search here went immediately to the most private files on the phone—those that required re-entry of the passcode to access, even after the phone was unlocked.

II. There was no reasonable individualized suspicion of an ongoing transnational offense to support the search in this case. The purported basis for the

---

implicated," and "the government must obtain a warrant based on probable cause." *Kolsuz*, 890 F.3d at 143.

search, on cross-examination, turned out to be nearly non-existent—a single ten-to-fifteen-month-old payment to a minor (who the sender may not have known was a minor) for an unknown reason coupled with travel to a country listed as similar to most others in the world for its efforts to combat child exploitation. Moreover, the court below made no finding that whatever suspicion existed related either to an ongoing offense or to a transnational offense—and there was no such evidence.

III. Finally, the search here was not permitted by good-faith reliance on binding precedent. This Court has expressly *not* decided whether manual searches of smartphones at the border require individualized suspicion. *Kolsuz*, 890 F.3d at 141, 146 n.5. And by requiring Mr. Belmonte Cardozo to provide the passcode to allow the search of his phone, CBP agents were not engaging in conduct this Court has approved—instead, they were testing the bounds of what the law *might* allow them to do.

STANDARD OF REVIEW

In reviewing the denial of a motion to suppress, this Court "review[s] the district court's legal conclusions de novo and its factual findings for clear error, considering the record evidence in the light most favorable to the Government." *United States v. Aigbekaen*, 943 F.3d 713, 719 (4th Cir. 2019) (citing *Kolsuz*, 890 F.3d at 141–42). Although the Court "review[s] the district court's findings of historical fact for clear error," it reviews "de novo the ultimate legal conclusion of

whether reasonable suspicion existed to justify police action." *United States v. Buster*, 26 F.4th 627, 630 (4th Cir. 2022) (internal citations and quotation omitted).

Further, "[b]ecause the Government conducted the challenged searches without warrants, it bears the burden of proving, by a preponderance of the evidence, that an exception to the warrant requirement applies." *Aigbekaen*, 943 F.3d at 719 (citing *United States v. Davis*, 690 F.3d 226, 262 (4th Cir. 2012)).

ARGUMENT

I. THE DISTRICT COURT CORRECTLY REQUIRED AN INDIVIDUALIZED SHOWING OF REASONABLE SUSPICION TO SEARCH A CELL PHONE AT THE BORDER.

A. Exceptions to the Warrant Requirement Are Narrowly Construed, and Their Scope Is Limited by the Justification Allowing an Exception.

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated[.]" U.S. Const. amend. IV. "Evidence gathered as fruit of an unreasonable search or seizure is generally inadmissible against a defendant." *United States v. Brown*, 401 F.3d 588, 592 (4th Cir. 2005) (citing *Taylor v. Alabama*, 457 U.S. 687, 694 (1982); *Wong Sun v. United States*, 371 U.S. 471, 484–86 (1963)). "'[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated

exceptions.'" *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)).

When the government invokes an exception to justify a warrantless search, the exception must be construed no more broadly than necessary to accommodate the justifications for the exception. *See id*. at 335 ("The safety and evidentiary justifications underlying *Chimel's* reaching-distance rule determine *Belton's* scope.") (referring to *Chimel v. California*, 395 U.S. 752 (1969), and *New York v. Belton*, 453 U.S. 454 (1981)). Exceptions to the Fourth Amendment's warrant requirement must be "jealously and carefully drawn," accompanied by "a showing by those who seek exemption that the exigencies of the situation made that course imperative." *Coolidge v. New Hampshire*, 403 U.S. 443, 455 (1971) (internal quotations and citations omitted). "Over and over again," the Supreme Court has "emphasized that the mandate of the Fourth Amendment requires adherence to judicial processes." *Katz*, 389 U.S. at 357 (internal quotation and alteration omitted).

Ultimately, *Gant* explains, the concerns underlying a warrant exception "define the boundaries of the exception." *Gant*, 556 U.S. at 339. To construe an exception to justify a warrantless search even when the concerns supporting the relevant warrant exception have dissipated would "untether the rule from [its] justifications." *Id.* at 343. An exception construed so broadly serves "no purpose

except to provide a police entitlement," which is "anathema to the Fourth Amendment." *Id.* at 347.

B. Following the Supreme Court's Admonition That Cell Phones Raise Unique Privacy Concerns, This Court Has Required Individualized Suspicion for Limited Forensic Searches of Cell Phones at the Border.

After *Gant*, the Supreme Court in *Riley v. California*, 573 U.S. 373 (2014), applied the same analysis to cell phones. Specifically, *Riley* held that a warrant is required to search a mobile phone incident to arrest because, while a "mechanical application" of the search-incident-to-arrest exception "might well support" a warrantless search of a cell phone following an arrest, the interests that justify searches incident to arrest—officer safety and destruction of evidence—do not. 573 U.S. at 386.

The Supreme Court's holding in *Riley* was premised on the unique Fourth Amendment implications of modern smartphones. *See id*. at 393–94:

> Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.
>
> One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical

> realities and tended as a general matter to constitute only a narrow intrusion on privacy. *See* Kerr, *Foreword: Accounting for Technological Change*, 36 Harv. J.L. & Pub. Pol'y 403, 404–405 (2013). Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in [*United States v. Chadwick,* 433 U.S. 1, 15 (1977)] rather than a container the size of the cigarette package in [*United States v. Robinson*, 414 U.S. 218 (1973)].

Four years later, the Court was presented with a related question in *Carpenter v. United States*, 585 U.S. 296 (2018)—whether a request under the Stored Communications Act directing a mobile phone service provider to produce 127 days' worth of cell site location information ("CSLI") required a warrant. CSLI is a time-stamped record of each time a particular cell phone connects to cellular network towers throughout a relevant time period. *Id*. at 300–301. Holding that a warrant was required, the Court noted "the deeply revealing nature of CSLI, [as well as] its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection." *Id*. at 320.

CSLI is less specific than GPS location information, but the Court nonetheless held that "[a]s with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."

Id. at 311 (citation and quotations omitted). Moreover, the Court noted, such location monitoring is even more intrusive than placing a GPS tracking device on a vehicle—a practice it had already held to require a warrant—because, "[w]hile individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.*

Accordingly, just as the Court in *Riley* departed from the otherwise applicable search-incident-to-arrest exception to hold that cell phones require heighted Fourth Amendment protection as compared to other items a person might carry upon arrest, so too did the Court in *Carpenter* depart from the "third party doctrine" to hold that the intrusiveness of CSLI collection was *sui generis*—it intrudes upon a mobile phone user's protected expectation of privacy even though the information was shared with and retained by a third party. *Id*. at 320.

This Court in *Kolsuz*, shortly before *Carpenter* was decided, recognized those same concerns when it limited the government's ability to perform suspicionless searches of cell phones at the border. Specifically, this Court held that, "in light of the Supreme Court's decision in *Riley*, a forensic border search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion" relating to "ongoing transnational crime." *Kolsuz*, 890 F.3d at 144. Importantly,

Kolsuz involved a non-password-protected device and a limited forensic search of only the data that would be seen by an ordinary user of the phone. *Id*. at 139, 145 n.4.

C. While This Court Has Not Addressed Manual Phone Searches at the Border, the Manual/Forensic Distinction Should Not Matter Because a Manual Search is Just as Privacy-Intrusive as a Forensic Search.

As already noted, the search in *Kolsuz* revealed exactly the same types of information that could have been reviewed through a manual search of the phone: "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." *Kolsuz*, 890 F.3d at 139. It did not include items an ordinary user could not see, such as "residual data of files that had been deleted by" the user. *Id.* at 145 n.4.

With respect to "the 'manual' searches performed in this case," the defense forensic expert William Jacob Green explained that they "were at least as extensive, if not more extensive, as the 'forensic' search performed in *Kolsuz*." J.A. 108. This was true not only because the manual searches allowed law enforcement to review all the same information, J.A. 108, but also because "the iPhones' internal capabilities for viewing and searching the phones' contents include powerful searching tools that allow a person with the phones' passcodes to access and search

all those items in the phone, exceeding the extraction method utilized in *Kolsuz*." J.A. 109.

By way of example, Mr. Green explained,

> the phones' internal capabilities … permit word-searching of every email, text message, and calendar entry. They allow a user to search for all photos depicting a specific person by pulling up a picture of that person and then searching for that same face in other pictures stored on the phone. Moreover, with respect to location history, each iPhone not only records and makes available to the user all of that history, sometimes incurring more than 60 days of locations, but it also arranges it by identifying "significant" or frequent locations and the times and dates the phone has been at those locations.

J.A. 109.[10]

To be sure, CBP makes and retains a digital copy of the electronic data on a device when it searches forensically—a step that is not required to perform a manual search. *See United States v. Saboonchi*, 990 F. Supp. 2d 536, 540 n.2 (D. Md. 2014) ("Imaging a hard drive is the first step of a forensic search and involves making a copy of a storage device that is known as an image, bitstream copy, or forensic copy.") (citation and quotations omitted). In practice, however, this is a minimal

[10] Indeed, native software on modern iPhones can even search a photo gallery by subject matter, by typing in a word such as "beach" or "sunset" to search for photos taken at the beach or of a sunset. *See iPhone User Guide: Search for Photos and Videos on iPhone*, APPLE, https://tinyurl.com/28bys7x6 (last accessed Oct. 15, 2025). This far exceeds the forensic search capabilities described in *Kolsuz*, where the software produced an 896-page report of the phone's contents. *Kolsuz*, 890 F.3d at 139.

distinction that should be given little weight. Considering that officers in a "manual" search can review every photo and video and word-search every written communication on a device, would they realistically spend any *additional* time during a forensic search reviewing the copy if—after performing all the same searches they would in a manual search—they had found nothing of interest? On the other hand, if they *do* find something of interest—in either a manual or forensic search—their next steps are identical (copying, reviewing and cataloging any evidence on the device). And, in the event of a forensic search that does not result in probable cause for seizure, CBP's policy is to promptly destroy its copy and return the device. *See* CBP Directive No. 3340-049A § 5.4.1.2 (Jan. 4, 2018), available at https://tinyurl.com/bdz88dzb. Accordingly, in all scenarios, the ultimate level of privacy intrusion is virtually identical whether law enforcement starts by making a forensic image of the device or not.

The principal argument the government made below for finding manual searches less intrusive than forensic searches fares no better. Specifically, the government argued that forensic searches use "external equipment" and "specialized software" while manual searches do not. J.A. 54 (citing *Aigbekaen*, 943 F.3d at 718 n.2). But the use of "external equipment" and "specialized software" is irrelevant to the Fourth Amendment inquiry, which turns on the degree of privacy intrusion implicated by the search. Consider, for example, listening to another person's voice

messages through wireless headphones versus listening through the phone itself. One method uses an external device with sophisticated wireless connectivity to translate an electronic file on the phone into an audible message—while the other uses the phone's native capabilities *to do the same thing*. The intrusion on privacy is the same.

For all these reasons, a number of federal courts have begun to note the fallacy of distinguishing between manual and forensic searches. *See United States v. Sultanov*, 742 F. Supp. 3d 258, 288 (E.D.N.Y. 2024) (finding that "the manual-vs.-forensic distinction is not a meaningful one for Fourth Amendment purposes."); *United States v. Alisigwe*, No. 22-cr-425, 2023 WL 8275923 at *5 (S.D.N.Y. Nov. 30, 2023) (concluding that a manual search of cell phone at border was nonroutine and required reasonable suspicion); *United States v. Gavino*, No. 22-cr-136, 2024 WL 85072 at *4 (E.D.N.Y. Jan. 7, 2024) (requiring reasonable suspicion for manual search of cell phone at border because *Riley* teaches that "even manual cell phone searches are intrusive").[11]

As the *Sultanov* court explained, citing the testimony of a CBP officer at the suppression hearing, "[a] manual search could be conducted by any number of officers, for any amount of time, and include a review of any type of content on the

[11] The author of *Sultanov* reiterated that holding in a more recent case. *See United States v. Robinson*, No. 23-cr-192, 2025 WL 1359352 at *1 (E.D.N.Y. May 9, 2025).

phone, including content that is password protected or encrypted." 742 F. Supp. 3d at 289. Moreover, the court continued,

> Once a CBP officer begins a manual search of an electronic device, the scope of the search is untethered from and unlimited by the original purpose of the search. A manual search can extend to logging into applications that are stored on the phone and reviewing the encrypted data saved in those applications, like, for example, financial transactions in a banking application. CBP can review not only the traveler's personal emails and text messages, but highly confidential documents that may be attached to those communications [citing, as examples, divorce and child-custody documents, sealed psychiatric records, and information about a not-yet-public corporate merger].

Id. (record citations omitted).

The government's answer to all this on the facts of this case—that the manual search was not particularly intrusive because it quickly led to contraband—is no answer at all. By that reasoning, a forensic search would, contrary to this Court's precedent, require no individualized suspicion as long as the searcher did what Officer Oliphant did here and went immediately to the hidden folders. Indeed, *Riley* involved searches incident to arrest, which presumably take place relatively soon after an arrest, but it made no exception for speedy manual searches. In fact, *Riley* rejected the government's proposed rule "that would restrict the scope of a cell phone search to those areas of the phone where an officer reasonably believes that information relevant to the crime … will be discovered." 573 U.S. at 399. Even in

the context of a manual search, the Court reasoned, such a rule would "impose few meaningful constraints on officers." *Id.*

Moreover, a speed-based rule is entirely unworkable. If an exception is made for "speedy" manual searches, at what point would a manual search become nonroutine? At 10-15 minutes, when the officer looks for "disguising applications" or a "hidden storage vault?" *See* J.A. 43. At 30 minutes, as the officer scrolls through direct messages in social media applications? J.A. 43. After an hour, as the officer reviews messages sent over text, WhatsApp and Signal? Another hour later, as the officer reads emails and attachments and meticulously reviews the user's location history? In any event, regardless of where the line is drawn, agents can access extremely sensitive information almost *immediately*, zeroing in on the places where people are likely to store their most sensitive information on the theory that those same locations are where evidence of crime might be found.

The circuits to have permitted suspicionless manual searches of electronic devices at the border do not address any of the above concerns and are unpersuasive. The Eleventh Circuit, for example, expressly applies a lower level of protection for electronic devices at the border than this Court, and as a result is unpersuasive here. *See United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018) (no suspicion required even for forensic searches). Three more are expressly premised on facts unlike those here—that the searches did not involve encrypted information or get

into files that are particularly private. *See United States v. Mendez*, 103 F.4th 1303, 1310 (7th Cir. 2024) (permitting suspicionless manual search that does not access "encrypted files" or "revealing nooks and crannies" of information on the phone); *see also Alasaad v. Mayorkas*, 988 F.3d 8, 19 (1st Cir. 2021) (upholding "basic" border searches of electronic devices that do not allow CBP to view "encrypted files"); *United States v. Castillo*, 70 F.4th 894, 897–98 (5th Cir. 2023) (same). And the Ninth Circuit in *Cano* simply reiterated an *en banc* pre-*Riley* holding, which was binding on the panel, for the proposition that "manual searches are reasonable without individualized suspicion, whereas the forensic examination of a cell phone requires a showing of reasonable suspicion." *United States v. Cano*, 934 F.3d 1002, 1016 (9th Cir. 2019) (citing *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013) (*en banc*)).

Finally, considering the border-protection-versus-privacy-intrusion calculus underlying border searches, the government's interest in interdicting digital contraband at the border is substantially lower than the border-enforcement interests implicated by physical contraband. *See United States v. Smith*, 673 F. Supp. 3d 381, 395 (S.D.N.Y. 2023) (explaining that because "digital data exists separate and apart from the physical cell phone on which it is stored, the Court doubts that the Government's interest in interdicting such 'digital contraband' as it exists on a specific device—when the exact same digital contraband likely is already stored

outside the device and available to its owner and others within this country—is genuinely comparable to the Government's interest in interdicting physical contraband."); *Sultanov*, 742 F. Supp. 3d at 285 ("Searching and seizing the data on a person's phone does not prevent that data, which the cell phone holder all but certainly obtained and/or stores outside the device, from entering and circulating within the country.") In other words, because digital contraband generally exists and travels "in the cloud," the government's interdiction of it at the border has much more to do with its "generalized interest in law enforcement and combatting crime," *Kolsuz*, 890 F.3d at 143, than with keeping it out of the country.

D. The Extraordinary Privacy Interests at Stake in Searching Modern Smartphones Are Too Great to Leave to Law Enforcement Officers' Unreviewable Discretion.

In the most recent quarter for which data is available, CBP searched 14,899 electronic devices during border encounters, for an annual rate of approximately 60,000 device searches per year.[12] This number has doubled in eight years.[13] And with CBP set to hire 5,000 new customs officers under a 2026 budget that is dramatically higher than its 2025 budget, those numbers seem certain to climb even

---

[12] *See Border Search of Electronic Devices at Ports of Entry*, U.S. CUSTOMS AND BORDER PROT., https://tinyurl.com/3cu27jm9 (last accessed October 19, 2025) (expand question entitled "How many border searches of electronic devices has CBP conducted?").

[13] *See CBP Statement on Border Searches of Electronic Devices*, U.S. CUSTOMS AND BORDER PROT. (Oct. 30, 2019), https://tinyurl.com/2ekpcrc9 (CBP conducted 30,200 border searches of electronic devices in Fiscal Year 2017).

faster in the coming years.[14] This represents a search rate that is greater by many orders of magnitude than the number of criminal cases that arise out of these searches.[15] CBP therefore appears to invasively search tens of thousands of cell phones each year belonging to innocent, ordinary travelers.

Moreover, because 90% of electronic-device searches conducted by CBP are non-forensic,[16] that means—if manual searches are permitted without any individualized suspicion—that these tens of thousands of invasive searches are performed at the unreviewable discretion of law enforcement. As this case shows, these searches can include the most private files people keep—those that are saved

---

[14] *See* Margy O'Herron, *Big Budget Act Creates "Deportation-Industrial Complex"*, BRENNAN CENTER FOR JUSTICE (Aug. 13, 2025), https://tinyurl.com/ycxf6ekd (noting that CBP budget is projected to increase by $65 billion over four years, from a $20 billion annual budget in fiscal 2025); Justin Doubleday, *DHS prepares for unprecedented spending surge under 'Big, Beautiful Bill'*, FEDERAL NEWS NETWORK (July 7, 2025), https://tinyurl.com/22mt3rnx (CBP projected to hire 5,000 new customs officers and 3,000 new border patrol agents).

[15] According to the United States Sentencing Commission, there were approximately 62,000 criminal cases sentenced under the federal Sentencing Guidelines in fiscal 2024, of which only 2.2% (about 1,400) involved child pornography. *See* U.S. SENT'G COMM'N, *Quarterly Data Report, Fiscal Year 2024* 2 (2024), https://tinyurl.com/4zkvkfhw. Based on a review of the reported cases involving border searches of electronic devices, child pornography offenses are far and away the most common type of criminal case arising from border searches of electronic devices (and, of course, border-search cases represent only a small portion of all child pornography offenses). Plainly, therefore, only a minuscule percentage of border searches of electronic devices result in criminal charges.

[16] *See Border Search of Electronic Devices at Ports of Entry*, *supra* note 12 (expand question entitled "How many border searches of electronic devices has CBP conducted?")

in hidden files, and/or are encrypted or password-protected. Permitting this level of privacy intrusion without any degree of suspicion would allow CBP officers to scroll through travelers' most intimate photos for any number of improper reasons—such as finding a traveler attractive and wondering if—like many Americans, *see supra* note 2—they have intimate photos stored on their phone.[17]

An additional reason that these searches are particularly intrusive, which was not at issue in *Kolsuz*, is CBP's requirement that travelers provide their passcodes. Regardless of whether Mr. Belmonte Cardozo had a Fifth Amendment right not to provide that information—an open question in this Circuit[18]—he was informed that

---

[17] This is not intended to impugn all CBP officers—but bad actors exist, and the risk of such misconduct is real. *See Customs and Border Protection Officer Arrested for Receiving Sexual Favors in Exchange for Allowing Aliens to be Smuggled Through His Lane*, FBI SAN DIEGO (Sep. 8, 2016), https://tinyurl.com/2mwk8h43; Julia Ainsley, *A Top Border Patrol Official Resigned After Allegedly Pressuring Female Employees for Sex, Officials Say*, NBC NEWS (Jan. 21, 2023), https://tinyurl.com/4jv4jndm; *Cracks in the Wall: When Border Watchdogs Turn Criminal*, TEXAS TRIBUNE (July 7, 2016), https://tinyurl.com/mskbsfjv (citing investigations of 140 CBP officers and other officials charged with border enforcement who had engaged in corruption, including at least several who did so for sex). These examples, of course, represent only those bad actors who have been identified.

[18] While this Court does not appear to have addressed whether compelled provision of a passcode to an electronic device violates the Fifth Amendment, other courts have found that it does. *See, e.g., United States v. Brown*, 125 F.4th 1186, 1204 (D.C. Cir. 2025) (holding that compelling owner to unlock cell phone—even where doing so requires thumb print rather than compelled provision of a code—violates Fifth Amendment); *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1345–46 (11th Cir. 2012) (concluding that the compelled provision of password violates Fifth Amendment because it forced owner to reveal

he was required to do so. And CBP was able to perform a manual search—and evade the *Kolsuz* requirement of individualized suspicion—only because it ordered Mr. Belmonte Cardozo to provide his passcode. But where the Fourth Amendment requires individualized suspicion—as it does in the case of limited forensic searches of cell phones at the border—it makes little sense to allow law enforcement to evade that requirement by ordering people to facilitate an equally intrusive search by a slightly different means.

II. THE SEARCH OF MR. BELMONTE CARDOZO'S SMARTPHONES WAS NOT SUPPORTED BY REASONABLE SUSPICION.

Given the significant privacy intrusion posed by manual searches, such searches should "be treated as nonroutine, permissible only on a showing of individualized suspicion." *Kolsuz*, 890 F.3d at 144. While this Court has refused to decide "whether more than reasonable suspicion is required," it has held that nonroutine searches of digital devices must be "based on at least reasonable suspicion." *Id*. at 148; *Aigbekaen*, 943 F.3d at 723 (assuming that "a warrantless

---

"the contents of his own mind."). And the Third Circuit has held that such information may be Fifth-Amendment-protected, but that compulsion may be permissible under the "foregone conclusion" doctrine where the testimonial aspect of providing the password does not reveal anything to law enforcement when it already has proof of the device's contents. *United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3d Cir. 2017). In this case, however, the compelled provision of the passcode was what allowed law enforcement to learn the phone's contents.

forensic search of a digital device at the border could be justified by reasonable suspicion").

Moreover, following the "general rule" that "the scope of a warrant exception should be defined by its justifications," this Court has emphasized that border searches must be justified by a connection to a border-specific offense. *Kolsuz*, 890 F.3d at 143. This Court reiterated in *Aigbekaen* that "the Government must have individualized suspicion of an offense that bears some nexus to the border search exception's purposes of protecting national security, collecting duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband." *Aigbekaen*, 943 F.3d at 721. Thus, the government cannot "invoke[] the border exception on behalf of its generalized interest in law enforcement and combatting crime." *Kolsuz*, 890 F.3d at 143.

A. The District Court Erred by Not Applying the Reasonable Suspicion Standard or Requiring a Nexus to an Ongoing Transnational Offense.

The district court noted that this Court in *Kolsuz* used the phrase "some measure of individualized suspicion," and relied on that as the standard to deny suppression. J.A. 166. Specifically, the court denied the motion upon finding that "Officer Oliphant did have some measure of individualized suspicion." J.A. 166; *see also Kolsuz*, 890 F.3d at 137 (finding that border search of electronic device requires "some measure of individualized suspicion," but declining to determine

"[w]hat precisely that standard should be"—reasonable suspicion or probable cause—because good-faith exception would have precluded suppression in *Kolsuz* regardless). Ultimately, *Kolsuz* did not decide whether the standard should be reasonable suspicion or probable cause—but it required *at least* reasonable suspicion. *Id.* at 148.

By relying on the phrase "some measure of individualized suspicion" as the governing standard, however, the ruling below failed to apply *Kolsuz's* actual holding as to the minimal level of suspicion required for nonroutine border searches: "some measure of individualized suspicion" amounting to: (i) "at least reasonable suspicion," (ii) of an "ongoing, transnational" crime. *Id*. at 137, 144, 148. Indeed, the district court never mentioned reasonable suspicion or the required nexus to a border crime in its ruling. J.A. 164–169 (the court mentioned the phrase "reasonable suspicion" only in its alternative holding about the good-faith exception and never mentioned the requirement of a nexus to an offense that is either "ongoing" or "transnational"). Nor did the court identify facts satisfying those requirements. J.A. 164–169.

By focusing solely on the requirement of "some" suspicion, the district court never grappled with the well-established meaning of the term "reasonable suspicion" as used in the Fourth Amendment context. To establish reasonable suspicion, an officer must be able to point to "specific and articulable facts which, taken together

with rational inferences from those facts, reasonably warrant" the intrusion "on the constitutionally protected interests of the private citizen." *Terry v. Ohio*, 392 U.S. 1, 21 (1968) (internal citation omitted). The reasonable suspicion standard looks to the "totality of the circumstances," and asks whether there is "a particularized and objective basis for suspecting the particular person stopped of criminal activity." *United States v. Cortez*, 449 U.S. 411, 417–18 (1981); *see United States v. Arvizu*, 534 U.S. 266, 273 (2002). Moreover, the standard depends on the facts specifically known to the officer at the time the search was initiated. *Terry*, 392 U.S. at 21–22 (reasonable suspicion turns on the facts available to the officer "at the moment of the seizure or the search").

Indeed, this Court has repeatedly "warned against the Government's proffering 'whatever facts are present, no matter how innocent, as indicia of suspicious activity,'" and has also been "deeply troubled by the way in which the Government attempts to spin … mundane acts into a web of deception." *United States v. Massenburg*, 654 F.3d 480, 482 (4th Cir. 2011) (quoting *United States v. Foster*, 634 F.3d 243, 248 (4th Cir. 2011)); *see United States v. Black*, 707 F.3d 531, 539 (4th Cir. 2013). "In practice [and as applied to a traveler], this typically means that 'an officer's articulated facts must in their totality serve to eliminate a substantial portion of innocent travelers before reasonable suspicion will exist.'" *United States*

v. Feliciana, 974 F.3d 519, 523 (2020) (quoting *United States v. McCoy*, 513 F.3d 405, 413 (4th Cir. 2008)).

B. The District Court Erred by Finding Reasonable Suspicion on the Basis of Vanishingly Thin Evidence.

Here, despite this Court's repeated warnings, the government takes entirely unsupported factual leaps, heaping inference upon inference, to support its contention that the facts known to Officer Oliphant established reasonable articulable suspicion of an ongoing transnational offense. The only individualized evidence was: (i) travel to Bolivia, a country similar in relevant respects to most countries in the world; and (ii) a financial transaction with a minor—who the sender may not have known to be a minor—which occurred for an unknown reason and in an unknown location, ten to fifteen months before the search.

To cobble that minimal record into reasonable suspicion of an ongoing transnational offense requires assumptions that the record cannot support. *First*, one would have to assume that the transaction was for a nefarious purpose rather than, for example, sending lunch money to a younger sibling with the memo "food and stuff." *Second*, one would have to assume that the nefarious purpose was sexual in nature rather than, say, buying marijuana. *Third*, one would have to assume that the nefarious sexual purpose related to an exchange of images rather than phone sex or an explicit text-message exchange or even a sexual encounter. *Fourth*, one would have to assume that those photos were not just sexually suggestive but child

pornography. *And fifth*, one would have to assume that those photos existed on the devices Mr. Belmonte Cardozo was carrying with him as he sought to enter the United States *ten to fifteen months later.*

The only other individualized evidence cited by the government—travel to Bolivia—fares no better. The report the government relied on for that point does not state that Bolivia has "increased rates of child sex trafficking," as Officer Oliphant testified at the suppression hearing. J.A. 153–154. Rather, it categorizes countries into tiers based on each country's efforts to eliminate trafficking and whether those efforts meet the standards outlined in the United States' Trafficking Victims Protection Act. *See* 2023 TRAFFICKING IN PERSONS REPORT, *supra* note 5, at 70. In other words, the report focuses on the Bolivian government's efforts to eradicate trafficking, but it says nothing about the *rates* of human trafficking in Bolivia and whether those rates are higher or lower than any other country. Moreover, Officer Oliphant did not even know whether the rate of sex trafficking in Bolivia was any higher than the rate in Virginia—which means that she had no evidence that passengers arriving from Bolivia had any higher likelihood of involvement in illicit activity than *any other traveler at Dulles.* In addition, Officer Oliphant did not dispute that in 2024 Bolivia was ranked in Tier 2 with the majority of other countries in the world, J.A. 152, so relying on the report's tier ranking system (even if that rating were based on the extent of sex trafficking, which it is not) would fail to

"eliminate a substantial portion of innocent travelers." *Feliciana*, 974 F.3d at 523 (citation omitted).

The government's two pieces of evidence, even taken together and viewed in the light most favorable to the government, are categorically weaker than was the case in *Aigbekaen*, 943 F.3d 713. In that case, the defendant's electronic devices were searched while he was entering the country approximately five weeks after a minor called 911 from a hotel to report that the defendant and another man "had transported her around Maryland, Virginia, and Long Island, New York; had posted ads of her on Backpage.com; and had trafficked her for sex." *Id.* at 717. Further investigation revealed that the defendant's phone number and email address were associated with the online posts advertising the minor for prostitution; rental car and hotel records also corroborated the minor's allegations and the defendant's involvement. *Id.* at 717–18. On the basis of all this information, and after learning that the defendant was traveling internationally, law enforcement requested that CBP conduct a border search of the defendant's electronic devices upon his return—which occurred approximately five weeks after the minor's 911 call. *Id.* at 718.

This Court held that the search in *Aigbekaen* required a warrant—it could not be justified even as a non-routine border search requiring individualized suspicion because its purpose was domestic law enforcement. In response to the government's

contention that sex trafficking "commonly involves cross-border movements," the Court explained:

> the general character of a crime may be relevant to an officer's reasonable suspicion that it involves a transnational component. But inherent in the notion of *individualized* suspicion is some evidentiary basis for what a specific crime *does* involve in the individual case at hand, not just what it 'commonly involves' as a general matter. Here, the Government has offered no reasonable basis to suspect that *Aigbekaen's* domestic crimes had any such transnational component.

943 F.3d at 721.

This was so even though the evidence known to law enforcement in *Aigbekaen* showed that "online prostitution ads" containing images of the minor had been posted just weeks before Mr. Aigbekaen's international travel. *Id.* at 717. This, as well as an "allegation from the manager of the hotel where the victim was recovered,"[19] lent support to the government's contention that the defendant "might be bringing contraband in the form of child pornography into the country." *Id.* at 718. Although the government argued that this "individualized suspicion" provided "the requisite nexus" to an ongoing transnational offense of importing child pornography, this Court disagreed. Instead, the Court held that "the Government

[19] Specifically, the hotel manager had informed law enforcement that he believed the defendant had been "filming sex acts with girls in their hotel room." *See United States v. Aigbekaen,* Supp. Br. of the Appellee, 2019 WL 268482 at *15 (Jan. 17, 2019).

lacked sufficient individualized suspicion of criminal activity with any nexus to the sovereign interests underlying the border search exception." *Id.* at 723–24.

This Court's holding was based largely on the weakness of the evidence supporting the inference that Mr. Aigbekaen was in possession of child pornography as he crossed the border. For example, the images of the minor in the prostitution ads may have been merely sexually suggestive rather than child pornography, and they may not have been on the defendant's devices when he crossed the border weeks after posting the ads. *Id*. at 717–18. And the evidence from the hotel manager was inconsistent. *Id.* at 723–24. But the evidence suggesting that Mr. Aigbekaen possessed child pornography as he was seeking to enter the United States was exponentially stronger than any inference in *this* case that Mr. Belmonte Cardozo possessed child pornography when he arrived at Dulles. Here, that evidence is that sometime between ten to fifteen months before traveling to Bolivia, Mr. Belmonte Cardozo had engaged in a financial transaction with a minor—whom the evidence does not even reveal he *knew* to be a minor—that a private company, for reasons undisclosed in the record, flagged as suspicious.

Finally, the fact that the government was engaged in an operation focused on interdicting CSAM at the time of the search does not support a finding of individualized suspicion. The government's decision to devote resources for increased investigation and enforcement is the opposite of a "particularized and

objective basis for suspecting a particular person stopped of criminal activity." *United States v. Peters*, 60 F.4th 855, 864 (4th Cir. 2023) (citation omitted). Indeed, even where a person is encountered in a "high-crime area"—which, unlike a decision to run an enforcement operation, is an objective fact specific to the encounter—that "fact [is] too generic and susceptible to innocent explanation" to establish reasonable suspicion. *Massenburg*, 654 F.3d at 488 (quoting *Illinois v. Wardlow*, 528 U.S. 119, 139 (2000)).

III. THE GOOD-FAITH EXCEPTION DOES NOT APPLY BECAUSE NO BINDING PRECEDENT AUTHORIZES SUSPICIONLESS PHONE SEARCHES OR ALLOWS LAW ENFORCEMENT TO REQUIRE TRAVELERS TO PROVIDE THEIR PASSCODES.

The good-faith exception provides that the fruits of "a search conducted in reasonable reliance on binding precedent [are] not subject to the exclusionary rule[.]" *Aigbekaen*, 943 F.3d at 725 (quoting *Davis v. United States*, 564 U.S. 229, 236–37 (2011)); *see also United States v. Baker*, 719 F.3d 313, 321 (4th Cir. 2013) (concluding that the good-faith exception applies where officer did "exactly what the law at the time said he could do"); *Davis*, 564 U.S. at 241 (holding that the exclusionary rule does not apply "when binding appellate precedent specifically *authorizes* a particular police practice") (emphasis in original); *United States v. Jenkins*, 850 F.3d 912, 920 (7th Cir. 2017) (explaining that "the *Davis* exception for good faith reliance on controlling precedent does not reach so far as to excuse mistaken efforts to extend controlling precedents") (citation omitted).

Thus, in *Aigbekaen*, where the search occurred in 2015, this Court did not apply the exclusionary rule because "[o]nly in 2018 did this court recognize that 'a search initiated at the border could become so attenuated from the rationale for the border search exception that it no longer would fall under that exception' and so require a warrant." 943 F.3d at 725 (quoting *Kolsuz*, 890 F.3d at 143). In other words, because "nonroutine" border searches had always been permitted on no more than reasonable suspicion—and because reasonable suspicion existed in *Aigbekaen*, albeit of a domestic offense—the search was authorized at the time it was conducted by pre-*Kolsuz* binding precedent. As a result, it was not subject to the exclusionary rule by the *Kolsuz* Court's later adoption of the ongoing-transnational-offense requirement. In this case, law enforcement was not relying on binding precedent authorizing their conduct. That is so for two reasons.

First, there is no binding precedent authorizing the suspicionless manual search of a cell phone at the border (or anywhere else). Indeed, *Kolsuz* identified that as an open question. 890 F.3d at 141 ("We … have no occasion to consider application of the border exception to manual searches of electronic devices, conducted at the border").

Below, after incorrectly contending that *Kolsuz* held that "the manual search of the phones at the airport did not require any individualized suspicion," J.A. 75, the government pivoted to reliance on an earlier case, *United States v. Ickes*, 393

F.3d 501 (4th Cir. 2005). Specifically, the government contended that, under *Ickes*, suspicionless searches of all electronic devices at the border are permissible within the Fourth Circuit. J.A. 65. But *Ickes* not only pre-dates modern smartphones—the first iPhone was introduced in 2007, seven years after the search in *Ickes*—it also rests on a holding directly contradicted by *Riley*—that electronic devices are no different than any other "cargo" a person carries. *Ickes*, 393 F.3d at 504. Moreover, if *Ickes* controlled the standard for manual searches of smartphones at the border even after *Riley* and *Kolsuz*, this Court in *Kolsuz* would not have treated the issue as an open question.[20]

In addition, *Ickes* does not "specifically authorize" suspicionless searches of digital devices at the border. In *Ickes*, the agents conducted a manual search of the defendant's laptop only *after* they found "photo albums of child pornography" in his van. *Id*. at 507. In other words, by the time the agents manually searched Mr. Ickes's computer, they already had probable cause to suspect he was carrying child sexual material. Thus, at most, *Ickes* authorizes border agents to manually search digital devices when "the traveler's conduct or the presence of other items in his possession

[20] Indeed, this Court did not overlook *Ickes* in *Kolsuz*. Instead, the Court discussed *Ickes* multiple times and yet still concluded that it was an open question "whether *Riley* calls into question the permissibility of suspicionless manual searches of digital devices at the border." *Kolsuz*, 890 F.3d at 146 n.5.

suggest the need to search further." *Id*. That holding does not authorize border agents to search digital devices without reasonable suspicion.

Second, there is no binding precedent authorizing law enforcement to order travelers to provide the passcodes to their devices as a condition of entering the country. As already noted, that question has not been addressed in this Circuit, but courts elsewhere have ruled that compelling travelers to provide their passcodes violates their Fifth Amendment rights. *See supra* note 18**.** And it allows the government to circumvent the requirements imposed by *Kolsuz*: instead of conducting a forensic search—which requires reasonable suspicion—the government can simply command a traveler to unlock their phone and then conduct an equally intrusive manual search. Indeed, the fact that the government obfuscated on this fact below—repeatedly claiming that Mr. Belmonte Cardozo provided the passcode "voluntarily" until the defense demonstrated otherwise, *see supra* note 1—suggests the opposite of good-faith reliance on precedent: that the government *knew* that its unlocking requirement was on thin ice.

Finally, the district court's ruling on the good-faith exception—as an alternative to its ruling that the search was supported by reasonable suspicion—should be given no deference because the court applied the wrong legal standard. The court identified no binding precedent authorizing the government's conduct but instead ruled that the search had "good faith protection" because it was "good law

enforcement practice." J.A. 169. That is not only not the law, but it is also an inherently subjective and backward-looking standard that this Court should not adopt.[21]

CONCLUSION

For the reasons argued above, the Court should reverse the District Court's Order denying Mr. Belmonte Cardozo's Motion to Suppress, vacate Mr. Belmonte Cardozo's convictions, and remand for further proceedings.

[21] Consider, for example, a case in which CBP searched a traveler's phone based on the same individualized suspicion that was present here, went immediately to the owner's most private files, and identified no contraband but instead found humiliating photos of the owner and/or his spouse. Had that traveler sued CBP for violation of his Fourth Amendment rights, it is doubtful that a court would be as likely to conclude that such an intrusive search, based on such minimal suspicion, was "good law enforcement practice."

Respectfully submitted,

GEREMY C. KAMENS
Federal Public Defender
for the Eastern District of Virginia

s/ Todd M. Richman

Todd M. Richman
Salvatore M. Mancina
Assistant Federal Public Defenders
Counsel for Appellant
1650 King Street, Suite 500
Alexandria, VA 22314
(703) 600-0800
Todd_Richman@fd.org
Sam_Mancina@fd.org

Dated: October 21, 2025

REQUEST FOR ORAL ARGUMENT

This case presents important and unresolved questions regarding border searches of electronic devices that have arisen repeatedly in this Court and in cases around the country. These issues impact not only the criminal matters in which they often arise, but also the rights of tens of thousands of international travelers each year whose privacy rights are implicated by the government practices at issue in this appeal. These issues may be more fully developed through oral argument, and counsel for appellant respectfully requests the same.

CERTIFICATE OF COMPLIANCE

1. This brief has been prepared using Microsoft Word for Office 365 software, Times New Roman font, 14-point proportional type size.

2. EXCLUSIVE of the table of contents, table of authorities, signature block, statement with respect to oral argument, and this certificate of compliance, this brief contains no more than 13,000 words, specifically 11,984 words.

I understand that a material misrepresentation can result in the Court's striking the brief and imposing sanctions. If the Court so requests, I will provide an electronic version of the brief and/or a copy of the word or line print-out.

October 21, 2025
Date

s/ Todd M. Richman
Todd M. Richman
Assistant Federal Public Defender