APPENDIX

Appendix A: Published opinion of the court of appeals
United States v. Belmonte Cardozo, 181 F.4th 461 (4th Cir. 2026)..... 1a

PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 25-4239

UNITED STATES OF AMERICA,

Plaintiff – Appellee,

v.

JOSE ALEJANDRO BELMONTE CARDOZO, a/k/a Jose Belmonte,

Defendant – Appellant.

KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY; REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS; AMERICAN CIVIL LIBERTIES UNION; ELECTRONIC FRONTIER FOUNDATION; NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS; ACLU OF MARYLAND; ACLU OF NORTH CAROLINA; ACLU OF SOUTH CAROLINA; ACLU OF VIRGINIA,

Amici Supporting Appellant.

Appeal from the United States District Court for the Eastern District of Virginia, at Alexandria. Leonie M. Brinkema, District Judge. (1:24-cr-00125-LMB-1)

Argued: May 8, 2026 Decided: July 13, 2026

Before DIAZ, Chief Judge, and AGEE and QUATTLEBAUM, Circuit Judges.

Affirmed by published opinion. Judge Quattlebaum wrote the opinion, in which Chief Judge Diaz and Judge Agee joined.

ARGUED: Todd M. Richman, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Alexandria, Virginia, for Appellant. James Reed Sawyers, OFFICE OF THE UNITED STATES ATTORNEY, Alexandria, Virginia, for Appellee. **ON BRIEF:** Geremy C. Kamens, Federal Public Defender, Salvatore M. Mancina, Assistant Federal Public Defender, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Alexandria, Virginia, for Appellant. Todd W. Blanche, Deputy Attorney General, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C.; Lindsey Halligan, United States Attorney and Special Attorney, Lauren Halper, Assistant United States Attorney, Jacqueline R. Bechara, Assistant United States Attorney, Alexandria, Virginia, Robert K. McBride, First Assistant United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Richmond, Virginia, for Appellee. Bruce D. Brown, Gabriel Rottman, Grayson Clary, REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, Washington, D.C.; Stephanie Krent, Raya Koreh, Scott B. Wilkens, Alex Abdo, Jameel Jaffer, Knight First Amendment Institute, COLUMBIA UNIVERSITY, New York, New York, for Amici The Knight First Amendment Institute at Columbia University and Reporters Committee for Freedom of the Press. Michael W. Price, Washington, D.C., Elizabeth Franklin-Best, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, Columbia, South Carolina; Nathan Freed Wessler, Esha Bhandari, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York; Sophia Cope, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California; Eden B. Heilman, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF VIRGINIA, Richmond, Virginia; Kristi L. Graunke, ACLU OF NORTH CAROLINA LEGAL FOUNDATION, Raleigh, North Carolina; David Rocah, AMERICAN CIVIL LIBERTIES UNION OF MARYLAND FOUNDATION, Baltimore, Maryland; Allen Chaney, AMERICAN CIVIL LIBERTIES UNION OF SOUTH CAROLINA FOUNDATION, Columbia, South Carolina, for Amici American Civil Liberties Union, Electronic Frontier Foundation, National Association of Criminal Defense Lawyers, ACLU of Maryland, ACLU of North Carolina, ACLU of South Carolina, and ACLU of Virginia.

QUATTLEBAUM, Circuit Judge:

Border searches do not require a warrant to be reasonable. And if a border search is routine, individualized suspicion is not required either. But law enforcement may not conduct a nonroutine border search without individualized suspicion. Under our precedent, forensic searches of cell phones are nonroutine. But what about manual searches? Today, we join all our sister circuits that have addressed this issue in holding that manual searches of cell phones at the border are routine and thus do not require individualized suspicion.

I.

On May 8, 2024, Jose Belmonte Cardozo traveled from Bolivia to the United States and landed at Washington Dulles International Airport. Though he didn't know it at the time, U.S. Customs and Border Protection Port Intelligence Officer Sara Oliphant was waiting for him.

When Belmonte Cardozo landed and presented himself for customs inspection, he produced two iPhones. Officer Oliphant asked Belmonte Cardozo to unlock the phones, and he complied.[1] She then opened the phones' photo galleries and toggled to their hidden galleries.[2] There, she found sexually explicit photos and videos of prepubescent girls. In

[1] Belmonte Cardozo mentions in his opening brief that there's an open question over whether compelling a defendant to provide his passcode violates the Fifth Amendment. In his reply brief, he clarifies he isn't pursuing a Fifth Amendment claim. So, we decline to address the question.

[2] According to an expert affidavit Belmonte Cardozo attached to his motion to suppress, iPhones give users the ability to store photos in a "hidden" folder within the phone's photo gallery. J.A. 110. Photos stored in the hidden folder only become visible when a user opens his photo application, uses a pulldown menu to choose hidden folders,

total, only about two minutes passed between Officer Oliphant taking possession of the phones and her discovering the illicit images. After discovering this material, CBP officers notified agents with the U.S. Department of Homeland Security, who arrived on the scene and arrested Belmonte Cardozo.

Later, the arresting agent filed a criminal complaint in the United States District Court for the Eastern District of Virginia, accusing Belmonte Cardozo of transporting child pornography. Eventually, a federal grand jury in that district indicted Belmonte Cardozo on five counts of sexual exploitation of a child in violation of 18 U.S.C. § 2251(a) and (e), two counts of coercion and enticement of a minor to engage in illegal sexual activity in violation of 18 U.S.C. § 2422(b), one count of transportation of child pornography in violation of 18 U.S.C. § 2252(a)(1) and (b)(1), one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1) and one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2).

Belmonte Cardozo moved to suppress the evidence recovered from the search of his cell phones. The district court held an evidentiary hearing, during which Officer Oliphant testified on the reasons she was suspicious of Belmonte Cardozo. After that, she was cross-examined on those reasons. And, after hearing this evidence, the district court denied

---

and re-enters the phone's passcode to see the contents of those folders. The expert opined that "[t]hese 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." J.A. 110. Based on this description of how the hidden folder works, we presume that Officer Oliphant was required to re-enter Belmonte Cardozo's passcode to unlock the hidden folders. The record is not entirely clear on how this happened, but Officer Oliphant testified she believed she asked Belmonte Cardozo to write down his passcode when she asked him to unlock the phones.

Belmonte Cardozo's motion to suppress from the bench. The court recognized that there was an open question about whether some level of individualized suspicion was needed for an officer to conduct a search of digital data on a cell phone at the border. However, it determined that even if "some measure of individualized suspicion" is required, Officer Oliphant had the requisite suspicion. J.A. 166. The court also commented that the search only took "about two minutes." J.A. 167. It added that, alternatively, Officer Oliphant acted in good faith.

Belmonte Cardozo and the government then entered into a conditional plea agreement pursuant to Federal Rule of Criminal Procedure 11(a)(2). Belmonte Cardozo pled guilty to all counts in the indictment but preserved his right to pursue this appeal of the denial of his motion to suppress. The district court accepted Belmonte Cardozo's plea and sentenced him to 18 years in prison, plus 25 years of supervised release.

This appeal, challenging the court's denial of the motion to suppress, followed.[3]

II.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. "As the text makes clear, the ultimate touchstone of the Fourth Amendment is reasonableness." *Riley v. California*, 573 U.S. 373, 381 (2014) (internal quotation marks omitted) (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)).

[3] We have jurisdiction under 28 U.S.C. § 1291. When examining the district court's denial of a motion to suppress, we review the district court's legal conclusions de novo and its factual findings for clear error, considering the evidence in the light most favorable to the government. *United States v. Aigbekaen*, 943 F.3d 713, 719 (4th Cir. 2019).

Reasonableness usually requires that law enforcement officers first obtain a warrant before conducting a search or seizure. *Id.* at 382. "This usual requirement, however, is subject to a number of exceptions."[4] *Birchfield v. North Dakota*, 579 U.S. 438, 456 (2016).

"Absent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement" by balancing the privacy implications against the underlying rationale for the search. *See Riley*, 573 U.S. at 385. In other words, we "assess[], on the one hand, the degree to which [the given type of search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *Id.* (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)).

This case sits at the intersection of two Fourth Amendment principles. First, individuals have heightened privacy expectations in their cell phones. Second, searches conducted by law enforcement officers at the border have long been recognized as reasonable under the Fourth Amendment. To decide how these principles fit together in this appeal, we start by explaining how cell phone searches are analyzed in other contexts. After that, we explore the rationale underlying the border search exception and how we have previously applied that exception to searches of electronic devices. And from there, we explain how these considerations come together to resolve this case.

[4] When the government conducts a search without a warrant, it must prove by a preponderance of the evidence that an exception applies. *Aigbekaen*, 943 F.3d at 719.

A.

1.

In *Riley*, the Supreme Court considered "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." 573 U.S. at 378. The Court reasoned that "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." *Id.* at 393. That's because cell phones have "immense storage capacity" and contain vast amounts of information about an individual. *Id.* at 393–94. This information is very personal, holding "for many Americans 'the privacies of life.'" *Id.* at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)); *see also Chatrie v. United States*, No. 25-112, 609 U.S. ---, 2026 WL 1855568, at *4 (June 29, 2026) (acknowledging that "the percentage of Americans who own smartphones has only increased" in the years since the Supreme Court decided *Riley*).

The Court then weighed these privacy concerns against the traditional justifications for permitting warrantless searches incident to arrest—officer safety and preventing concealment or destruction of evidence. *Riley*, 573 U.S. at 386–98. In balancing these interests, the Court determined neither of the justifications for a search incident to arrest permitted the warrantless search of a cell phone. *Id.* at 387–91. It explained that "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape." *Id.* at 387. And it reasoned there's no risk an arrestee could delete incriminating data off a cell phone once the officers secure it away from the arrestee's person. *Id.* at 388.

Thus, the Court concluded that a warrant is "generally required" before police can search the digital information on cell phones after an arrest. *Id.* at 401. But it also pointed out that "even though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone." *Id.* at 401–02.

2.

This case involves the border search exception to the warrant requirement, not the search incident to arrest exception. Warrantless searches at the border are not inherently "unreasonable" under the Fourth Amendment. *See Boyd*, 116 U.S. at 623. That's because of the "long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country." *United States v. Ramsey*, 431 U.S. 606, 616 (1977). Indeed, the same Congress that proposed the Fourth Amendment to the states for ratification in 1789 also enacted our nation's first customs statute, which gave customs officials broad authority to board vessels suspected of transporting concealed goods. *Id.* at 616–17. Thus, "[s]ince the founding of our Republic, Congress has 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). In short, the government's "paramount interest in protecting[] its territorial integrity" by "preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152–53 (2004).

What's more, an individual's privacy expectations at the border are less than they would typically be in the interior. *Montoya de Hernandez*, 473 U.S. at 539–40. So, the balance of these expectations against the government's heightened interests at the border justifies the border search exception. *See id.*; *Flores-Montano*, 541 U.S. at 152–54. And the border search exception applies not only at the border but also at its "functional equivalent," such as an international airport. *Almeida-Sanchez v. United States*, 413 U.S. 266, 272–73 (1973).

Even so, there are limits to warrantless searches at the border. One limit depends on whether the search is routine. *United States v. Kolsuz*, 890 F.3d 133, 138 (4th Cir. 2018). Routine border searches are reasonable without individualized suspicion, but nonroutine searches are reasonable only when justified based on some level of individualized suspicion. *Id.* at 138, 146–47. Typically, this means border officials must have reasonable suspicion, which in turn requires that "officials at the border . . . have a 'particularized and objective basis for suspecting the particular person'" of committing an offense. *Montoya de Hernandez*, 473 U.S. at 541–42 (quoting *United States v. Cortez*, 449 U.S. 411, 417 (1981)). *But see Kolsuz*, 890 F.3d at 137 (declining to resolve whether a nonroutine forensic cell phone search at the border must be supported by reasonable suspicion or probable cause).[5] And that offense must "bear[] some nexus to the border search exception's

[5] We said in *Kolsuz* that something beyond reasonable suspicion might be required to support nonroutine border searches of electronic devices, but we ultimately did not decide that question. *See* 890 F.3d at 137. Even so, no circuit, including us, has ever "read *Riley* to require more than reasonable suspicion to support even the most intrusive electronics search at the border." *United States v. Mendez*, 103 F.4th 1303, 1309 (7th Cir. 2024) (collecting cases).

purposes of protecting national security, collecting duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband." *United States v. Aigbekaen*, 943 F.3d 713, 721 (4th Cir. 2019).

So, what's a nonroutine search? The Supreme Court has suggested that "'highly intrusive searches' that implicate especially significant 'dignity and privacy interests,' as well as destructive searches of property and searches carried out in 'particularly offensive' manners" are nonroutine. *Kolsuz*, 890 F.3d at 138 (quoting *Flores-Montano*, 541 U.S. at 152, 154 & n.2). But the Court has never held that any search of someone's property—as opposed to an invasive search of someone's person—is a nonroutine search. *See Flores-Montano*, 541 U.S. at 155–56 ("While it may be true that some searches of property are so destructive as to require [suspicion], this was not one of them."); *see also United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018); *Aigbekaen*, 943 F.3d at 728 (Richardson, J., concurring). This suggests there's a "high bar" to clear before a property search becomes nonroutine. *Aigbekaen*, 943 F.3d at 728 (Richardson, J., concurring).

3.

With these principles in mind, we turn to searches of electronic devices at the border. This is not our first occasion to address that issue.

In *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005), law enforcement stopped the defendant, who was traveling across the Canadian border in his van. *Id.* at 502. During an inspection, an officer found marijuana, a copy of an arrest warrant for the defendant and albums containing child pornography. *Id.* at 503. The officer also confiscated the defendant's laptop computer and 75 disks containing child pornography. *Id.* Law

enforcement searched the contents of the computer, and the defendant admitted it stored child pornography. *Id.* The defendant argued the First Amendment carves out an exception to the border search doctrine for "expressive material."[6] *Id.* at 506. In addressing that issue, we didn't grapple with whether the search was a routine border inspection. *See id.* at 502. Instead, we started from the premise—in other words, we basically assumed—that the search was routine before rejecting the defendant's First Amendment argument. *See id.* In reaching that conclusion, we reasoned that the First Amendment does not prevent the government from conducting warrantless border searches to further its important interest in protecting the country from illicit material coming in. *Id.* at 505–07.

More recently, in *Kolsuz*, we held that forensic searches of cell phones at the border are nonroutine and require "some measure of individualized suspicion." 890 F.3d at 137. In that case, a Turkish citizen was traveling home through Dulles. *Id.* at 138. When CBP officers inspected his bags, they discovered firearms parts that could not be removed from the United States without a license. *Id.* at 139. And the defendant admitted he did not have such a license. *Id.* The officers moved the defendant to a secondary inspection area and confiscated his iPhone. *Id.* They manually searched the phone by scrolling through the defendant's recent calls and text messages. *Id.* They then transported the phone to a facility four miles from the airport, where they searched the phone forensically by attaching it to data extracting equipment. *Id.* The forensic search lasted a full month and "yielded an 896-

[6] The defendant also argued the search exceeded the officer's statutory authority. *Id.* at 503–04. We rejected that argument, but our reasoning on that point is less relevant to Belmonte Cardozo's appeal. *See id.* at 505.

page report that included [the defendant's] personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of [the defendant's] physical location down to precise GPS coordinates." *Id.*

The defendant moved to suppress the information uncovered in the forensic search of his phone, but the district court denied that motion. *Id.* at 139–40. On appeal, the defendant argued that, even under the border exception, "the forensic search of his phone constituted a nonroutine border search unsupported by the type of reasonable suspicion required to justify such searches."[7] *Id.* at 144 (citation modified). We first determined that, under *Riley*, "a forensic border search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion." *Id.* That's largely because the forensic report on the defendant's phone produced a tremendous amount of personal information. *Id.* at 144–46. Next, we noted that "[n]onroutine searches are permitted under the border exception, so long as they are accompanied by the appropriate level of individualized suspicion." *Id.* at 146–47. But rather than determining whether the officers had the necessary level of suspicion, we affirmed the denial of the motion to suppress based on good faith. *Id.* at 148. Even if the forensic search in fact required probable cause, we held that "it was reasonable for the CBP officers who conducted the forensic analysis of [the

[7] The defendant also argued the forensic search of his cell phone wasn't covered by the border exception at all because the search was conducted several miles from the airport, over the course of a month and was not related to intercepting contraband that was in the process of crossing international borders. *Id.* at 142–43. We rejected this argument because "the link between the search of [the defendant's] phone and the interest that justifies border searches was sufficient to trigger the border exception on any account of a 'nexus' requirement," as the officers were attempting to find evidence of his attempts to illegally export firearms parts. *Id.* at 143.

defendant's] phone to rely on the established and uniform body of precedent allowing warrantless border searches of digital devices that are based on at least reasonable suspicion." *Id.*

In reaching this decision, we distinguished *Ickes*. In a footnote, we reasoned that "*Ickes* approved a manual, on-site inspection of computer contents that would be accessible to any user, and did not address the use of the sophisticated forensic search methods at issue [in *Kolsuz*]." *Id.* at 146 n.5. But because the defendant did "not challenge the initial manual search of his phone at Dulles, we ha[d] no occasion [t]here to consider whether *Riley* calls into question the permissibility of suspicionless manual searches of digital devices at the border." *Id.*

B.

Finally, with that background, we come to the question left open by *Kolsuz* and presented by this appeal—are manual cell phone searches at the border routine or nonroutine?

Belmonte Cardozo argues they are nonroutine. He relies primarily on the privacy interests inherent in cell phones that *Riley* and *Kolsuz* identified. According to Belmonte Cardozo, because of the advanced search features on modern iPhones, the level of privacy intrusion in a manual search is essentially the same as in the nonroutine forensic search in *Kolsuz*. For example, he points out that iPhones allow a user to type in keywords and will produce images saved on the phone associated with those words and that users can search for images of individual people and the phone will produce saved images of those people. In addition, Belmonte Cardozo argues the government has less interest in searching digital

data at the border than it does physical contraband. He contends that, because digital contraband could enter the country through electronic means, there is no specific reason to conduct a cell phone search to prevent digital contraband from crossing the border.

The government, in contrast, argues manual cell phone searches at the border are routine. In fact, it insists *Ickes* compels that result. And *Riley*, the government adds, did not abrogate *Ickes*.

Neither Belmonte Cardozo nor the government is right. As for the government's point, *Ickes* doesn't control our decision here. It may be true that we effectively treated the border search in *Ickes* as a routine search. *See* 393 F.3d at 502, 505–07 & n.1; *see also Kolsuz*, 890 F.3d at 146 n.5. But we did so as a starting point before evaluating whether the First Amendment places restrictions on routine border searches for expressive content. *See Ickes*, 393 F.3d at 506–07. We never grappled with whether the search of an electronic device at the border was routine or nonroutine. Thus, our assumption about that antecedent proposition is not binding. *See Payne v. Taslimi*, 998 F.3d 648, 654 (4th Cir. 2021) ("[W]here we 'assum[e] without deciding the validity of antecedent propositions' those assumptions 'are not binding in future cases that directly raise the questions.'" (second alteration in original) (quoting *United States v. Norman*, 935 F.3d 232, 241 (4th Cir. 2019))).

We also disagree with Belmonte Cardozo's argument about the government's interest in digital data at the border. Even if digital contraband can cross the border electronically, that does not reduce the government's interest in interdicting digital contraband when it crosses the border on a smartphone or other device. *See United States*

v. Nkongho, 107 F.4th 373, 381 (4th Cir. 2024) (recognizing the "critical" need for forensic border searches in "preventing cross-border crime and the importation of contraband . . . such as child pornography"); *United States v. Cano*, 934 F.3d 1002, 1014 (9th Cir. 2019) ("The contents may be digital when they are on the phone, but the physicality of the phone itself and the possibility that the phone's contents can be printed or shared electronically gives border officials sufficient reason to inspect it at the border."). In such circumstances, the government retains its "paramount interest" in preventing contraband from entering the country, which is "at its zenith at the international border."[8] *See Flores-Montano*, 541 U.S. at 152–53.

And the privacy expectations one has in the digital contents of his or her cell phones do not overcome the government's interests. It is true that individuals have heightened privacy interests in such information. *See Riley*, 573 U.S. at 393–98. And it is also true that those very interests prompted us to find that forensic cell phone searches at the border are nonroutine. *See Kolsuz*, 890 F.3d at 146. But for several reasons, manual searches are different.

First, a person does the looking in a manual search, not a machine. *See, e.g.*, *id.* at 139; *Aigbekaen*, 943 F.3d at 718 n.2. In a manual search, an officer opens the device, scrolls through it and reads what any user would see. In a forensic search, an officer connects the device to outside hardware or software, copies its contents and analyzes the copy.

[8] Besides, the government has more than an interest in what enters the country; it has an interest in who enters. *Flores-Montano*, 541 U.S. at 152 ("The Government's interest in preventing the entry of *unwanted persons and effects* is at its zenith at the international border." (emphasis added)).

Second, the breadth of the searches is different. A manual search ends when the officer's time, patience and attention give out. A forensic search is comprehensive. The outside tool sweeps the whole device. To illustrate this difference, recall that Officer Oliphant searched Belmonte Cardozo's phone for approximately two minutes before uncovering the illicit images. In contrast, the forensic search in *Kolsuz* took a month and produced close to 900 pages of information. *See* 890 F.3d at 139. Border officials simply lack the time and manpower that it would take to manually search electronic devices in a way that would recover the amount of information obtainable from forensic searches.

Third, a manual search sees only what a user can access on a device. A forensic search recovers more—deleted files, cached fragments, location histories, system logs and metadata the owner never knew he kept. As Belmonte Cardozo conceded at oral argument, some forensic searches can produce information that has been deleted from a phone. Oral Argument at 5:50–6:07. Thus, a forensic search exposes not just what an ordinary user would consider to be the contents of a phone; it opens a window beyond. *See Aigbekaen*, 943 F.3d at 718 n.2 (observing that a cell phone forensic search is "'a powerful tool' capable of . . . 'unlocking password-protected files, restoring deleted material, and retrieving images viewed on websites'" (quoting *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc)); *see also Cotterman*, 709 F.3d at 962–63 (drawing distinction between forensic and manual searches of a laptop because the forensic search "is akin to reading a diary line by line looking for mention of criminal activity—plus looking at everything the writer may have erased").

And fourth, a manual search is subject to an officer's fading memory or imperfect notes. A forensic search is not—it creates a copy the government may be able to keep. *Cf. Carpenter v. United States*, 585 U.S. 296, 312 (2018) (reasoning that, prior to the advent of technology in modern cell phones, an officer's personal effort to track a person's movement was "limited by a dearth of records and the frailties of recollection"). The copy is a permanent, portable and searchable duplicate of the device. The government can carry it from the border, study it at leisure and search it for keywords. A forensic search does not end at the border crossing; it begins there.

Considering the differences in forensic and manual searches and balancing the government's interest in preventing contraband from entering the country at the border with individuals' privacy expectations in the data in their cell phones, we hold that manual cell phone searches are routine border searches that do not require individualized suspicion. The concerns particular to forensic searches identified in *Kolsuz* are not present here. And the differences between manual and forensic searches compel a different result.

In reaching this conclusion, we have company. In fact, every one of our sister circuits to have considered the issue has reached the same result. *See United States v. Mendez*, 103 F.4th 1303, 1310 (7th Cir. 2024) ("We therefore agree with the consensus among circuits that brief, manual searches of a traveler's electronic device are 'routine' border searches requiring no individualized suspicion."); *United States v. Castillo*, 70 F.4th 894, 898 (5th Cir. 2023) ("We see no reason to disagree with our sister circuits. Accordingly, we hold that no reasonable suspicion is necessary to conduct the sort of routine manual cell phone search at the border that occurred here."); *Alasaad v. Mayorkas*,

988 F.3d 8, 19 (1st Cir. 2021) ("We thus agree with the holdings of the Ninth and Eleventh Circuits that basic border searches [of electronic devices] are routine searches and need not be supported by reasonable suspicion."); *Cano*, 934 F.3d at 1014 ("Accordingly, we hold that manual searches of cell phones at the border are reasonable without individualized suspicion, whereas the forensic examination of a cell phone requires a showing of reasonable suspicion."); *Touset*, 890 F.3d at 1233–35 (finding that the Fourth Amendment does not require individualized suspicion to justify a forensic search of a cell phone at the border and rejecting distinction between routine and nonroutine border searches of property); *see also United States v. Xiang*, 67 F.4th 895, 899–900 (8th Cir. 2023) (recognizing that "[n]o Circuit has held that the government must obtain a warrant to conduct a routine border search of electronic devices").

None of this is to say that there aren't limits to manual searches. Were the government to devote the manpower and time needed to conduct lengthy manual searches in a way that would deprive an individual of their phone for extended periods of time, other Fourth Amendment principles may come into play. For example, "a search which is reasonable at its inception may violate the Fourth Amendment by virtue of its intolerable intensity and scope." *Terry v. Ohio*, 392 U.S. 1, 18 (1968). But the facts of this case do not test those limits. [9]

[9] The parties also dispute whether the facts known to Officer Oliphant supported individualized suspicion and whether the good faith exception applies. Because we ultimately find this search did not require individualized suspicion, we decline to address whether the search was supported by individualized suspicion. That said, even if individualized suspicion were required and even if Officer Oliphant did not have the

III.

Because we find that manual searches of cell phones at the border are routine border searches which don't require individualized suspicion, the judgment of the district court is,

AFFIRMED.

requisite level of suspicion, suppression would still not be appropriate based on Officer Oliphant's good-faith reliance "on the established and uniform body of precedent" that allows suspicionless manual searches of cell phones at the border. *Kolsuz*, 890 F.3d at 148.