

In the
United States Court of Appeals
For the Seventh Circuit

No. 23-1460

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

MARCOS MENDEZ,

Defendant-Appellant.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 16-cr-163 — **Mary M. Rowland**, *Judge*.

ARGUED DECEMBER 5, 2023 — DECIDED JUNE 10, 2024

Before HAMILTON, BRENNAN, and ST. EVE, *Circuit Judges*.

ST. EVE, *Circuit Judge*. Marcos Mendez was passing through customs at O'Hare International Airport after a trip abroad when a customs agent pulled him aside for inspection, unlocked and scrolled through his cell phone, and found child pornography in the photo gallery. Customs agents then seized the phone, downloaded its contents, and discovered additional illicit images and videos of children.

After the district court denied Mendez’s motion to suppress this evidence, Mendez pled guilty to producing child pornography but preserved this appeal of the district court’s suppression-motion ruling. He now argues that the searches of his phone, in light of the Supreme Court’s decisions in *Riley v. California*, 573 U.S. 373 (2014), and *Carpenter v. United States*, 585 U.S. 296 (2018), required a warrant, probable cause, or at least reasonable suspicion.

The “longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless ‘reasonable’ has a history as old as the Fourth Amendment itself.” *United States v. Ramsey*, 431 U.S. 606, 619 (1977). That history leads us to join the uniform view of our sister circuits to hold that searches of electronics at the border—like any other border search—do not require a warrant or probable cause, and that the kind of routine, manual search of the phone initially performed here requires no individualized suspicion. We affirm.

I. Background

A. Factual Background

Just shy of midnight on February 20, 2016, Marcos Mendez landed at O’Hare International Airport following a trip to Ecuador. He was traveling alone. Along with his baggage, Mendez carried with him three electronic devices: a personal cell phone, a work phone, and a work iPad.

Customs and Border Protection (“CBP”) had issued a child-pornography-related “lookout” for Mendez based on his arrest record and prior travel history. Mendez had a 2010 arrest relating to indecent solicitation of a child and child pornography, leading to a 2011 conviction for endangering the

No. 23-1460

3

life or health of a child. Additionally, CBP previously had inspected Mendez in 2014 after he returned from Mexico. During that inspection, he claimed to have been kidnapped, robbed of his electronic devices, and told to leave the country. And on this particular trip, Mendez was returning from Ecuador, which CBP officers classified as a potential child-trafficking source country. Mendez also fit the profile for child-pornography offenders: a single adult male traveling alone.

Together, this information prompted CBP Investigating Officer Richard Callison to pull Mendez aside for secondary inspection after his arrival at O'Hare. Within the first thirty minutes of the inspection, Mendez gave Callison his cell phone and its passcode. Callison manually unlocked the phone and navigated to its camera roll. There he found thousands of pornographic images, including what appeared to be child pornography. Using the phone's passcode, Callison also opened a protected application called "iSafe," where he discovered more illicit images.

Callison then moved Mendez to a private location, where he conducted a more extensive, "forensic" examination of Mendez's devices. CBP agents used a data extraction technology called "DOMEX" (Document and Media Exploitation) to download a copy of the devices' photos and videos. The forensic examination took about two hours and revealed more child pornography.

Officers seized Mendez's cell phone but released Mendez, who, in the days after his arrest, remotely wiped the contents of his phone and traveled by car into Mexico with his mother. Meanwhile, a Homeland Security Investigations ("HSI") team extracted the metadata—creation dates, geolocation information, and so on—from the files that had earlier been

downloaded from Mendez's cell phone. That data revealed that several of the child pornography images were taken near Mendez's residence in Rosemont, Illinois.

B. Procedural Background

A grand jury indicted Mendez on two counts of producing child pornography, in violation of 18 U.S.C. § 2251(a), one count of transporting child pornography, in violation of 18 U.S.C. § 2252A(a)(1), and one count of possessing child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). He was extradited to the United States in January 2020.

Mendez moved to suppress the evidence found on his cell phone, arguing the searches violated the Fourth Amendment because they were unsupported by either a probable-cause supported warrant or reasonable suspicion. After an evidentiary hearing in which Officer Callison and other investigating officers testified, the district court denied the motion. Relying in large part on our decision in *United States v. Wanjiku*, 919 F.3d 472 (7th Cir. 2019), the district court held that the searches did not violate the Fourth Amendment because customs agents had reasonable suspicion by the time they began looking through Mendez's phone.

Mendez pled guilty to one count of producing child pornography but preserved his right to appeal the district court's suppression ruling. He received a 300-month sentence, followed by a ten-year term of supervised release. We now consider that preserved issue, reviewing the district court's findings of fact for clear error and questions of law de novo. See *United States v. Ostrum*, 99 F.4th 999, 1004 (7th Cir. 2024).

No. 23-1460

5

II. Analysis

The Fourth Amendment commands that searches and seizures be reasonable. U.S. Const. amend. IV. Ordinarily, “[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.” *Riley*, 573 U.S. at 382.

One such exception is the border search exception. “Congress, since the beginning of our Government, ‘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.’”¹ *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004) (quoting *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985)). The government’s unquestionable authority to search persons and effects at the border is rooted in “the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country.” *Ramsey*, 431 U.S. at 616; see also *id.* at 619 (“Historically such broad powers have been necessary to prevent smuggling and to prevent prohibited articles from entry.”); *Flores–Montano*, 541 U.S. at 152 (noting that the border exception rests on the government interest in “preventing the entry of unwanted persons and effects”). The “Fourth Amendment balance between the interests of the Government and the privacy right

¹ We treat the customs area of O’Hare International Airport as “the functional equivalent of an international border for the purpose of inspecting persons and articles arriving on international flights.” *Wanjiku*, 919 F.3d at 480 (citing *United States v. Yang*, 286 F.3d 940, 944 (7th Cir. 2002)); see also *Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973).

of the individual is ... struck much more favorably to the Government at the border.” *Montoya de Hernandez*, 473 U.S. at 540. When the government acts under its “inherent authority to protect ... its territorial integrity,” its interest is “at its zenith.” *Flores-Montano*, 541 U.S. at 152–53. In contrast, a traveler’s expectation of privacy at the border is simply “less.” *Montoya de Hernandez*, 473 U.S. at 539.

Accordingly, border searches have long been exempted from warrant and probable cause requirements, and ordinarily “are reasonable simply by virtue of the fact that they occur at the border.” *Flores-Montano*, 541 U.S. at 152–53 (quoting *Ramsey*, 431 U.S. at 616). “Routine” searches of people and effects at the border—which have included examining the contents of a person’s purse, wallet, or pockets, *United States v. Carter*, 592 F.2d 402 (7th Cir. 1979), opening mail, *see Ramsey*, 431 U.S. at 620, and disassembling and reassembling a vehicle’s fuel tank, *see Flores-Montano*, 541 U.S. at 155—are “per se reasonable” and require no particularized suspicion at all. *Yang*, 286 F.3d at 944 (citing *Ramsey*, 431 U.S. at 616); *see also Montoya de Hernandez*, 473 U.S. at 538 (“Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant.”); *United States v. Johnson*, 991 F.2d 1287, 1291 (7th Cir. 1993).

Even highly intrusive, so-called “non-routine” border searches need only reasonable suspicion. *See Montoya de Hernandez*, 473 U.S. at 541. But the Supreme Court has recognized this “non-routine” category only in searches of a suspect’s person. It held, for example, that a 16-hour detention for monitored bowel movement of a person suspected of “smuggling contraband in her alimentary canal” requires reasonable

No. 23-1460

7

suspicion given the personal dignity and privacy interests at stake. *Id.* at 541. And in this circuit, “we have confronted border searches and seizures that we characterized as *arguably* non-routine”—including pat downs, partial strip searches, visual body cavity searches, and the dismantling of luggage—and have applied the reasonable suspicion standard. *Wanjiku*, 919 F.3d at 482–83 (emphasis added); *see also Yang*, 286 F.3d at 944, 949; *Kaniff v. United States*, 351 F.3d 780, 784–85 (7th Cir. 2003); *Johnson*, 991 F.2d at 1291–94.

Routine or otherwise, searches at the border “never” require a warrant or probable cause. *Ramsey*, 431 U.S. at 619 (“There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause.”). At most, border searches require reasonable suspicion. *See Wanjiku*, 919 F.3d at 481; *United States v. Molina-Isidoro*, 884 F.3d 287, 291 (5th Cir. 2018) (“For border searches both routine and not, no case has required a warrant.”). In more than 200 years of border search precedent, neither the Supreme Court nor we have ever found a border search unconstitutional.

Mendez argues that *Riley* and *Carpenter* upended that precedent by recognizing that cell phones fundamentally differ from other types of personal effects. *See Riley*, 573 U.S. at 393; *Carpenter*, 585 U.S. at 318. Yet our caselaw highlights why neither case supports altering the long-settled rule exempting border searches from warrant and probable cause requirements: *Riley* and *Carpenter* had nothing to do with the border context. *See Wanjiku*, 919 F.3d at 484; *United States v. Wood*, 16 F.4th 529, 533 (7th Cir. 2021) (“Given the context-specific

nature of the Fourth Amendment, *Riley* is not readily transferable to scenarios other than the one it addressed.”).²

Rather, *Riley* involved the search incident to arrest exception and “carefully tailored its analysis to that context.” *Wood*, 16 F.4th at 533. What is unreasonable after arrest may be perfectly reasonable at customs, as *Riley* itself anticipated. *See Riley*, 573 U.S. at 401–02 (“[O]ther case-specific exceptions may still justify a warrantless search of a particular phone.”); *see also New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985) (Fourth Amendment reasonableness “depends on the context within which a search takes place.”). A border search is

² *Wanjiku* and a later decision, *United States v. Skaggs*, 25 F.4th 494 (7th Cir. 2022), resolved the identical issue of electronic device searches at customs under the Fourth Amendment’s good faith exception to the warrant requirement. “[N]o court,” we observed in *Wanjiku*, “had ever required more than reasonable suspicion for any search at the border.” 919 F.3d at 479. And because we found that law enforcement had reasonable suspicion to search the defendant’s phone, “[g]iven the state of the law at the time of the[] searches,” we concluded that law enforcement had “an objectively good faith belief that their conduct did not violate the Fourth Amendment.” *Id.* at 485–86. While we left the merits of the Fourth Amendment issues open in those cases, we go on to reach those merits issues here to provide clarity to law enforcement and the public on the burgeoning practice of electronic device searches. *See Molina-Isidoro*, 884 F.3d at 293 (Costa, J., specially concurring) (“Courts should resist the temptation to frequently rest their Fourth Amendment decisions on the safe haven of the good-faith exception, lest the courts fail to give law enforcement and the public the guidance needed to regulate their frequent interactions.”); *United States v. Bosyk*, 933 F.3d 319, 332 n.10 (4th Cir. 2019) (“[W]hen a Fourth Amendment case presents a novel question of law whose resolution is necessary to guide future action by law enforcement officers and magistrates, there is sufficient reason for [a court] to decide the violation issue before turning to the good-faith question.” (alterations in original) (quoting *Illinois v. Gates*, 462 U.S. 213, 264 (1983) (White, J., concurring))).

fundamentally different from a search incident to arrest, not least because “the Fourth Amendment’s balance of reasonableness is qualitatively different at the international border,” where the government’s interest in protecting its territorial integrity is at its peak and travelers’ expectations of privacy are diminished. *Montoya de Hernandez*, 473 U.S. at 538; cf. *United States v. 12 200-Ft. Reels of Super 8MM. Film*, 413 U.S. 123, 125 (1973) (“Import restrictions and searches of persons or packages at the national borders rest on different considerations and different rules of constitutional law from domestic regulations.”). Underlying the Court’s decision in *Riley* was the fact that neither of the search incident to arrest exception’s twin concerns—preventing harm to officers and destruction of evidence—“ha[d] much force with respect to digital content on cell phones.” *Riley*, 573 U.S. at 386. Here, in contrast, we agree with the First Circuit that “given the volume of travelers passing through our nation’s borders, warrantless electronic device searches are essential to the border search exception’s purpose of ensuring that the executive branch can adequately protect the border.”³ *Alasaad v. Mayorkas*, 988 F.3d 8, 17 (1st Cir. 2021).

While Mendez argues that cell phone searches are untethered to the border search doctrine’s justifications, this case

³ We have twice declined to extend *Riley* beyond the search incident to arrest exception: to parolee searches in *Wood*, 16 F.4th at 533, and to consent searches in *United States v. Thurman*, 889 F.3d 356, 366 n.9 (7th Cir. 2018) (finding in the consent-search context that “*Riley* d[id] not affect our holding” because “[a]lthough the Court discussed the unique nature of modern cell phones as unparalleled repositories for personal information, it did not address the consent-based exception to the warrant requirement”).

illustrates that cell phones *can* contain the contraband the border search doctrine means to intercept: here, digital contraband in the form of child pornography. See *United States v. Cano*, 934 F.3d 1002, 1014 (9th Cir. 2019) (“The best example [of digital contraband] is child pornography.”). The government’s interest in detecting child pornography at the border is just as strong as its interest in intercepting firearms, narcotics, or any other prohibited item.⁴ See *United States v. Touse*, 890 F.3d 1227, 1235 (11th Cir. 2018) (“‘[Digital]’ child pornography poses the same exact ‘risk’ of unlawful entry at the border as its physical counterpart.”). That digital contraband like child pornography can pass into the country electronically or be accessed remotely does little to diminish the government’s interest in preventing its physical entry into the country. See

⁴ Although the scope of a search conducted under an exception to the warrant requirement must be “commensurate with its purposes,” *Arizona v. Gant*, 556 U.S. 332, 339 (2009), the Ninth Circuit is the only circuit to cabin the border search exception to detecting contraband itself. Compare *Cano*, 934 F.3d at 1019 (holding that “border officials are limited to searching for contraband only”), with *United States v. Levy*, 803 F.3d 120, 124 (2d Cir. 2015) (noting that CBP officers “have the authority to search and review a traveler’s documents and other items at the border when they reasonably suspect that the traveler is engaged in criminal activity, even if the crime falls outside the primary scope of their official duties.”), and *United States v. Xiang*, 67 F.4th 895, 900 (8th Cir. 2023) (adopting the Second Circuit’s “more sensibl[e]” position), and *Alasaad*, 988 F.3d at 20 (“[T]he border search exception’s purpose is not limited to interdicting contraband; it serves to bar entry to those ‘who may bring anything harmful into this country.’” (emphasis in original) (quoting *Montoya de Hernandez*, 473 U.S. at 544)), and *United States v. Aigbekaen*, 943 F.3d 713, 721 (4th Cir. 2019) (finding the purposes of the exception to be “protecting national security, collecting duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband”).

No. 23-1460

11

id. (“If anything, the advent of sophisticated technological means for concealing contraband only heightens the need of the government to search property at the border.”); *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971) (“Customs officers characteristically inspect luggage and their power to do so is not questioned ... ; it is an old practice and is intimately associated with excluding illegal articles from the country.”). And although it was not the case here, a border search of a cell phone could also facilitate the doctrine’s goal of “reasonably requiring one entering the country to identify himself as entitled to come in.” *Carroll v. United States*, 267 U.S. 132, 154 (1925).

No circuit court has read *Riley* to require more than reasonable suspicion to support even the most intrusive electronics search at the border. See *United States v. Castillo*, 70 F.4th 894, 897–98 (5th Cir. 2023) (“[W]hen it comes to manual cell phone searches at the border, our sister circuits have uniformly held that *Riley* does not require either a warrant or reasonable suspicion.”); *Molina-Isidoro*, 884 F.3d at 293 (5th Cir. 2018); *Xiang*, 67 F.4th at 900 (8th Cir. 2023) (“*Riley* involved a different Fourth Amendment exception, searches incident to arrest. No Circuit has held that the government must obtain a warrant to conduct a routine border search of electronic devices.”); *Alasaad*, 988 F.3d at 17 (1st Cir. 2021) (“*Riley* does not command a warrant requirement for border searches of electronic devices nor does the logic behind *Riley* compel us to impose one.”); *Cano*, 934 F.3d at 1015 (9th Cir. 2019); *Touset*, 890 F.3d at 1234 (11th Cir. 2018) (“Although the Supreme Court stressed in *Riley* that the search of a cell phone risks a significant intrusion on privacy, our [caselaw makes] clear that *Riley*, which involved the search-incident-to-arrest exception, does not apply to searches at the border.”); *United States*

v. Vergara, 884 F.3d 1309, 1312–13 (11th Cir. 2018) (“Border searches have long been excepted from warrant and probable cause requirements, and the holding of *Riley* does not change this rule.”); *United States v. Kolsuz*, 890 F.3d 133, 147 (4th Cir. 2018). We join our sister circuits to hold that a border search of a cell phone or other electronic device requires neither a warrant nor probable cause.

The question remains whether the agent’s manual search of Mendez’s phone—scrolling through its photo gallery—was a routine search permissible without any suspicion or a “non-routine” search requiring reasonable suspicion. Mendez contends that because electronic devices carry potentially vast troves of sensitive and personal information, we should treat *all* electronic device searches as intrusive border searches requiring at least reasonable suspicion. *Riley* itself involved a manual phone search and no doubt indicates that all cell phone searches are intrusive to some degree, but the privacy concerns such searches implicate “are nevertheless tempered by the fact that the searches are taking place at the border.” *Alasaad*, 988 F.3d at 18. Moreover, manual electronic searches at the border are typically “brief procedure[s]”—here, around thirty minutes—practically limited in intrusiveness by the fact that the customs agent cannot download and peruse the phone’s entire contents. Instead, they must physically scroll through the device, making it less likely for an agent to tap into the revealing nooks and crannies of the phone’s metadata, encrypted files, or deleted contents. *Flores-Montano*, 541 U.S. at 155; compare *United States v. Cotterman*, 709 F.3d 952, 960 (9th Cir. 2013) (en banc) (pre-*Riley* decision finding the legitimacy of a suspicion-less “quick look and unintrusive” manual laptop search “not in doubt”), with *Kolsuz*, 890 F.3d at 136 (requiring reasonable suspicion for a month-long,

No. 23-1460

13

off-site forensic analysis that yielded a nearly 900-page report cataloguing the phone's data).

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. See *Castillo*, 70 F.4th at 897–98 ("[W]hen it comes to manual cell phone searches at the border, our sister circuits have uniformly held that *Riley* does not require either a warrant or reasonable suspicion."); *Alasaad*, 988 F.3d at 19 ("[B]asic border searches [of electronic devices] are routine searches and need not be supported by reasonable suspicion."); *Cano*, 934 F.3d at 1016 ("[M]anual searches of cell phones at the border are reasonable without individualized suspicion."); *Touset*, 890 F.3d at 1233; *Kolsuz*, 890 F.3d at 146 n.5 (describing *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005), as "treat[ing] a [basic] search of a computer as a routine border search, requiring no individualized suspicion").

The only point of divergence among the circuits is whether more intrusive, forensic electronic device searches require individualized suspicion. Compare *Touset*, 890 F.3d at 1231 (no suspicion required for forensic electronics search), with *Cano*, 934 F.3d at 1016 (reasonable suspicion required). We need not resolve this issue today because this case does not require it. The valid manual search of Mendez's phone revealed child pornography. So, even if the extensive forensic searches that followed required reasonable suspicion, customs agents had that and more once they found illicit images and videos of children on Mendez's phone during the routine search.

AFFIRMED