In the

United States Court of Appeals

For the Seventh Circuit

No. 18-1973

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

DONALD WANJIKU,

Defendant-Appellant.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 1:16-cr-00296-1 — **Elaine E. Bucklo**, *Judge.*

ARGUED NOVEMBER 7, 2018 — DECIDED MARCH 19, 2019

Before ROVNER, SYKES, and BARRETT, *Circuit Judges*.

ROVNER, *Circuit Judge.* Donald Wanjiku pled guilty to one count of transportation of child pornography in violation of 18 U.S.C. § 2252A, but he retained his right to appeal the district court's denial of his motion to suppress the primary evidence against him. That evidence included photographs and videos recovered from his cell phone, laptop and external hard drive

during a warrantless border search at O'Hare International Airport. We affirm.

I.

On June 9, 2015, Wanjiku arrived at O'Hare after a trip to the Philippines. Unbeknownst to Wanjiku, Customs and Border Patrol ("CBP") and Homeland Security Investigations ("HSI") were together conducting a criminal investigation dubbed "Operation Culprit" at the airport that day. Operation Culprit targeted certain individuals returning from three countries known to investigators for "sex tourism" and sex trafficking, including the sex trafficking of children. The investigators developed a list of initial criteria to identify individuals of interest to Operation Culprit: (1) U.S. citizen (2) men (3) between the ages of eighteen and fifty or sixty (4) returning from the Philippines, Thailand, or Cambodia (5) traveling alone (6) with a prior criminal history. Along with an unspecified number of other passengers from the eight to ten flights that investigators were monitoring that day, Wanjiku met all of the initial screening factors. That is, he is a U.S. citizen male, then aged forty-one, returning from the Philippines, traveling without any apparent companion, with a prior arrest.

Investigators sought to whittle down the resulting list by further investigating these travelers before they arrived at O'Hare. Using government databases[1] and publicly available

---

[1] The investigators used a DHS system called "TECS" to conduct their research. TECS allows investigators to search other databases linked to CBP (continued...)

social media, they determined that Wanjiku's prior arrest was for contributing to the delinquency of a minor,[2] that this was his third trip to the Philippines in two years, that this trip was sixty days in length, and that he had no apparent affiliation with the Philippines other than these trips. For example, they were unable to find business or family ties to the Philippines for Wanjiku. The investigators determined that Wanjiku had booked a prior flight using an email address that incorporated the name "Mr. Dongerous," which heightened their suspicions based on their belief that this was a play on the word "dong," which is vulgar slang for penis.[3] Using that email address, they searched Facebook and found a public Facebook page associated with that address. The person in the profile picture

---

[1] (...continued)
including the National Criminal Information Center ("NCIC"), the National Automated Immigration Lookout System ("NAILS"), and the Arrival and Departure Information System ("ADIS"), among others. Together, these databases provide information about passengers' arrival and departure records, criminal histories, immigration status, and email addresses and phone numbers used to book travel.

[2] CBP Officer Adam Toler testified at the suppression hearing that he could not recall when the arrest had occurred and did not know how it was resolved. He also did not know the specific allegations underlying it.

[3] During cross-examination, Wanjiku's counsel suggested that the email address was a play on Wanjiku's first name, "Don." Wanjiku placed no evidence in the record regarding the origin of the email address, and of course, it is possible for the address to be a play on both "Don" and "dong." As we will discuss below, in determining whether a search violates the Fourth Amendment, a court evaluates only how a reasonable officer would have interpreted this information.

(whom they believed to be Wanjiku) was wearing a mask of the type that one wears to a masquerade ball. Photos of "friends" on that page appeared to be "very young" relative to Wanjiku's age.[4] The investigators for Operation Culprit found all of this suspicious enough to warrant sending Wanjiku to a more thorough secondary inspection on his arrival at the airport.[5]

After Wanjiku passed through the primary inspection point and was referred to the secondary inspection area in Baggage Hall A, CBP Officer Toler met Wanjiku for a more thorough secondary inspection. Toler testified that, at the secondary inspection area, he typically would take the traveler's bags and then obtain a binding declaration from that person. He would then ask what the traveler was doing outside of the United States, obtain a story about the trip, and then go through the traveler's bags to see if the contents of the bags corroborated the traveler's answers. Toler candidly testified at the suppression hearing that investigators had already decided to inspect the contents of Wanjiku's cell phone and other electronic devices before he reached the secondary inspection point

---

[4] Agent Toler testified that Wanjiku had approximately fifty to one hundred Facebook friends, and approximately half were younger. When pressed by the court at the suppression hearing to describe the ages of the friends, Toler responded, "I'm just guessing at age. Looked not in their forties." R. 59, Tr. at 51. He later added, "I'm not sure exactly what the age is; but they weren't in their 30s." R. 59, Tr. at 52.

[5] In total, Operation Culprit investigators selected twenty-three or twenty-four individuals for secondary inspection from the two to three thousand passengers arriving on the targeted flights that day. R. 59, Tr. at 16.

(indeed, before he reached the primary inspection point) on the basis of the information that they had gathered prior to his arrival. Nevertheless, before those devices were actually inspected, Wanjiku gave the investigators additional cause for concern. For openers, at the primary inspection point, the officer interacting with Wanjiku indicated in notes to the secondary inspector that Wanjiku was "evasive for questioning."

At the secondary inspection area in Baggage Hall A, Wanjiku came to Toler's attention even before Toler could begin his usual inspection process. Toler saw Wanjiku leave the line of persons awaiting inspection, something Toler had never seen a passenger do before. As Toler later learned from an Immigration and Customs Enforcement ("ICE") agent, Wanjiku left Baggage Hall A and walked approximately two hundred feet away and across an exit corridor to a bathroom in Baggage Hall B, even though there was an identically marked bathroom much closer in Baggage Hall A. Wanjiku left his luggage in the line when he took this walk and an ICE agent escorted him back to the line.

At the beginning of the inspection, Toler asked Wanjiku why he had left the line. Wanjiku replied that he had heat stroke and needed to use the bathroom. Toler noted that Wanjiku was sweating profusely in the air conditioned hall, was shifting his weight, and seemed visibly nervous. Toler then asked Wanjiku about the trip itself, and Wanjiku said he had been visiting friends in the Philippines for two months. In response to Toler's questions, Wanjiku also revealed that he had left the U.S. with $6000 and was returning with just a few hundred dollars. He had stayed at the home of the friends he

was visiting. Because Wanjiku had reported on a Customs Declaration form that he was not bringing in items exceeding $800 in value and because he had said he was staying with friends, Toler asked him how he had spent more than $5000 during the trip. Wanjiku gave vague and evasive answers, saying only that his friends had shown him around the country. He also told Toler that he sometimes sent or gave money to the family he stayed with in order to help their child attend school. He went to the Philippines, he said, in part to make sure his money was being put to good use. Toler asked where Wanjiku traveled in the Philippines and he would not elaborate, saying only that his friends showed him around the country. Toler went through the list of questions that a traveler normally must answer on the standard Customs Declaration form, including whether he was bringing in more than $10,000 in currency, food, cell cultures, snails, or gifts, among other things.

After obtaining a binding declaration from Wanjiku, Toler prepared to inspect Wanjiku's two large bags and single carry-on bag. He asked if the bags belonged to Wanjiku and whether Wanjiku himself had packed them. Wanjiku responded affirmatively to both questions. In response to Toler's questions, he denied that there were any sharp objects in the bags that could possibly poke, cut or hurt Toler as he went through the bags. Toler and another agent then opened the bags. They set aside Wanjiku's cell phone, laptop and portable hard drive for later inspection. In one bag, Toler found a pocket full of receipts, including multiple receipts for hotel stays. Most were for one-night stays, and two were for one-night stays at the same hotel approximately one week apart. Because Wanjiku

had previously told Toler that he stayed with friends, Toler asked what the hotel receipts were for. Wanjiku said that his friend showed him around the country and these receipts were from those trips. That answer heightened Toler's suspicions both because Wanjiku had previously given the address of the friend as the place he stayed and because Toler deemed it unusual to stay at the same hotel twice in the span of a week if a person is traveling around the country. He asked Wanjiku about the dual receipts for the same hotel specifically and Wanjiku would not elaborate, instead asking Toler whether it was illegal to go around the country or have a friend show him around the country.

Toler next found a pocket containing syringes and condoms, which upset him because Wanjiku had denied that the bags contained sharp objects, putting Toler at risk of injury. When asked about the syringes, Wanjiku explained that he had medication in his other bag. The injectable medication recovered from the other bag was to treat low testosterone. The second bag also contained oxycodone and OxyContin pills, a narcotic pain medication. The medications raised additional red flags for Toler because he believed that testosterone was a "sexually specific" substance related to "male genitalia." R. 59, Tr. at 34. Moreover, both medications were in the name Donald Kwiatkowski, not Donald Wanjiku. Wanjiku explained that he had changed his name, and offered a social security card issued in his prior name to support his claim.

After completing this check of Wanjiku's bags, Toler turned his attention to the cell phone. The phone was password-protected, and Toler began by asking Wanjiku to unlock the phone. Wanjiku initially resisted but relented when Toler told

him that everything was searchable at the border and that the phone would be seized, unlocked by a "lab," and examined whether or not Wanjiku unlocked it. Toler took the unlocked phone and manually scrolled through the pictures. Within a minute, he found several pictures of Wanjiku lying in bed with another man who was in his underwear. Although Toler twice referred to the other person in the photos as a "man," he also testified at the suppression hearing that he was uncertain of the age of the person pictured.[6] Toler then turned the phone over to HSI because the HSI forensics team was better trained than he to identify child pornography.

Agent Kevin Gerlock of HSI was the computer forensic coordinator on the scene at O'Hare that day. HSI agents used forensic software to "preview" Wanjiku's cell phone and hard drive while Wanjiku waited at the secondary inspection area. Gerlock explained that "EnCase" software was used first to preview Wanjiku's external hard drive. EnCase allows a search of the contents of a hard drive without modifying or destroying any of the information contained on the device. A preview, Gerlock testified, involved looking only at allocated space on the device, essentially items catalogued by the device's operating system in files. In contrast, a full forensic examination of a device would copy every bit of memory in the device and would reveal items that had been deleted or placed in

---

[6] After examining the pictures herself, the district judge specifically found that Toler's claim that he could not determine the age of the individual pictured was credible. Notably, though, the district court did not rely on the presence of these photos in determining whether the agents possessed reasonable suspicion to search Wanjiku's electronic devices.

hidden areas of memory. A preview generally takes one to three hours to complete. A full forensic examination could take months. The agents used software to inspect the devices in order to avoid damaging the devices or altering the data on the devices.[7]

Agent Mark Bowers performed the forensic preview on the hard drive, which was neither password-protected nor encrypted. Bowers used the EnCase software to view photographs and videos stored on the device. The preview took less than an hour and revealed six videos of suspected child pornography. The file names for the videos included references to the ages of the children portrayed and terms known to the agents to be associated with child pornography. For example, one file was labeled "pthc-15yogirlteaching12yoboys." Gerlock explained that "pthc" is known by the agents to be an abbreviation for "preteen hardcore." Gerlock, having seen the videos, confirmed that the titles were in fact descriptive of the content.[8]

---

[7] Agent Gerlock explained that electronic devices sometimes track the time and date that a person last looked at a photo and that by manually scrolling through the device, the agents might inadvertently alter that kind of data. Gerlock also testified that cell phones sometimes contain apps that will alter data or even delete it if someone accesses the data manually. The software allowed the agents to see the photos and videos without altering the data in any way. R. 59, Tr. at 95, 99. None of the searches altered the data or harmed the devices.

[8] After a warrant was obtained, a full forensic examination of the hard drive was conducted, revealing approximately twenty-two videos of child pornography.

The second preview search performed by forensics officers at the airport that day was of Wanjiku's Samsung cell phone.[9] In this instance, Officers Keith Smith and Marci Landri used "Cellebrite" and "XRY" software to review photos and videos stored on the phone. As with the hard drive, the search did not include deleted or hidden files. The agents did not attempt to inspect email, text messages or similar data, instead confining the searches to photographs and videos. The fourteen photographs of child pornography that were found that day were stored on a small memory card inserted into the phone rather than in the memory of the phone itself. This removable "micro SD" memory card was neither password-protected nor encrypted.

The agents lacked the necessary equipment to preview the laptop at the airport. Because child pornography had already been discovered on two of Wanjiku's electronic devices, the laptop was taken to an HSI lab where it was previewed approximately one week later. The laptop preview took under three hours, and agents again restricted the search to photographs and videos, not searching for deleted or hidden files. Child pornography was also recovered from the laptop. For each electronic device, the photographs and videos that were

---

[9] The preview search of the phone was performed over a two-day period. At the airport on the first day, Smith discovered photographs indicative of child pornography. Because the agents' workday was then at an end, the phone was taken to the agents' office the next day to preview videos. At that point, because child pornography photos had already been found on the phone, the device could not clear customs and would not be returned to the traveler. Together, the preview searches of the phone lasted under two hours.

suspected to be child pornography were copied to a compact disk and entered into evidence at the suppression hearing.[10]

On the basis of the photographs and videos discovered on Wanjiku's electronic devices during these warrantless searches at the border, he was charged with one count of transportation of child pornography, in violation of 18 U.S.C. § 2252A(a)(1). Wanjiku moved to suppress the evidence collected during the searches of his electronic devices at the border, arguing that it was improper for the agents to insist that Wanjiku unlock the phone, and that searches of electronic devices are non-routine border searches that require reasonable suspicion or, arguably, a warrant.[11] The government countered that the preview examinations of the devices were routine searches that may be conducted at the border without any suspicion whatsoever. In the alternative, the government asserted that the agents possessed reasonable suspicion based both on information known to them before Wanjiku arrived at O'Hare and information developed during routine inspection and questioning, and that no court had required more than reasonable suspicion for

---

[10] Although full forensic searches were completed for all three devices after a warrant was obtained, we confine ourselves to the airport preview searches because those provided the basis for obtaining the warrant. If the initial searches withstand constitutional scrutiny, then the full forensic searches also stand up.

[11] In his reply brief on the Motion to Suppress, Wanjiku clarified his position by arguing that "a reasonable suspicion standard should apply, but also … in the wake of *Riley v. California*, 134 S. Ct. 2473 (2014), there are grounds for a higher standard, namely probable cause and a warrant." R. 50, at 1. Wanjiku mainly contended in the district court that the agents lacked reasonable suspicion to search his electronic devices.

even a non-routine border search. The district court found that the information known to the agents at the time they searched Wanjiku's devices was sufficient to trigger a reasonable suspicion that he was involved in the kind of criminal activity targeted by Operation Culprit. The court therefore denied the motion to suppress the fruits of the border search, and Wanjiku pled guilty conditionally, retaining his right to challenge the district court's suppression ruling on appeal.

II.

On appeal, Wanjiku contends that, in the wake of the Supreme Court's decisions in *Riley v. California*, 134 S. Ct. 2473 (2014), and *Carpenter v. United States*, 138 S. Ct. 2206 (2018), border searches of electronic devices may be conducted only with a warrant supported by probable cause. In the alternative, if the applicable standard is reasonable suspicion, he contends that the facts known to the officers when they decided to search his electronic devices were not sufficient to give rise to reasonable suspicion. The government takes the position that no individualized suspicion is needed for a routine border search of electronic devices. In the alternative, the government argues that if probable cause is now required under *Riley* and *Carpenter*, suppression would not be warranted under the good faith doctrine. Finally, the government maintains that if reasonable suspicion is the appropriate standard for border searches of electronic devices, that standard was met here. In reviewing a district court's denial of a motion to suppress, we review findings of fact for clear error and questions of law *de novo*. *United States v. Velazquez*, 906 F.3d 554, 557 (7th Cir. 2018); *United States v. Borostowski*, 775 F.3d 851, 863 (7th Cir. 2014).

The primary positions staked out by the parties could not be more starkly contrasted. The defendant argues that nothing less than a warrant authorizes a search of electronic devices at the border. The government asserts that it may conduct these searches without any particularized suspicion at all. In the end, though, we need not adopt either of these positions, and indeed may avoid entirely the thorny issue of the appropriate level of suspicion required. Instead, we affirm the district court's denial of the motion to suppress because these agents acted in good faith when they searched the devices with reasonable suspicion to believe that a crime was being committed, at a time when no court had ever required more than reasonable suspicion for any search at the border.

A.

Two months before the First United States Congress proposed the Bill of Rights, it enacted the first customs statute, granting customs officials "'full power and authority' to enter and search 'any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed . . ..'" *United States v. Ramsey*, 431 U.S. 606, 616 (1977) (quoting section 24 of Act of July 31, 1789, c. 5, 1 Stat. 29). Approximately one hundred years later, the Supreme Court noted that the statute allowing searches of ships and vessels and the seizure of goods "concealed to avoid the duties payable on them" had been passed by the same Congress that proposed the Fourth Amendment. That timing made clear "that the members of that body did not regard searches and seizures of this kind as 'unreasonable,' and they are not embraced within the prohibition of the amendment." *Boyd v. United States*, 116 U.S. 616, 623 (1886). *See also Ramsey*, 431 U.S.

at 616 ("searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border").

This is because the "Government's interest in 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 (2004). The Court has linked this longstanding, congressionally-granted, search-and-seizure authority to two main purposes: to allow the regulation of 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). *See also United States v. 12 200-Foot Reels of Super 8mm Film*, 413 U.S. 123, 125 (1973) (noting that broad powers to conduct searches of persons and packages at national borders are "necessary to prevent smuggling and to prevent prohibited articles from entry."); *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 in this case; it is an old practice and is intimately associated with excluding illegal articles from the country."); *Carroll v. United States*, 267 U.S. 132, 154 (1925) (although it would be intolerable if a prohibition agent were allowed to stop all cars on the chance of finding liquor, "[t]ravelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in.").

Although neither party cited in their appellate briefs the statutory authority under which CBP carried out the searches here, modern analogues of the customs law passed by the First Congress include 19 U.S.C. § 482 (search of vehicles and persons); 19 U.S.C. § 1467 (special inspection, examination, and search); 19 U.S.C. § 1496 (examination of baggage); 19 U.S.C. § 1581 (boarding vessels); and 19 U.S.C. § 1582 (search of persons and baggage; regulations).[12] The customs area of O'Hare International Airport, located in Chicago, is treated as the functional equivalent of an international border for the purpose of inspecting persons and articles arriving on international flights. *United States v. Yang*, 286 F.3d 940, 944 (7th Cir. 2002) ("O'Hare Airport is an international gateway into the United States, and incoming passengers from international ports are subject to border searches because the airport is the functional equivalent of an international border."). *See also Almeida–Sanchez v. United States*, 413 U.S. 266, 272–73 (1973) ("a search of the passengers and cargo of an airplane arriving at a St. Louis airport after a nonstop flight from Mexico City would clearly be the functional equivalent of a border search."). Wanjiku does not contest generally the statutory right of border agents to search his belongings at the airport for contraband but instead argues that, once agents have determined that an electronic device is not being used as a container to smuggle a prohibited substance (*e.g.* an explosive or illegal drugs), they must have a warrant or at least reasonable

---

[12] In the district court, the government cited and relied upon 19 U.S.C. § 1581. R. 49, at 7, n.8.

suspicion to examine the electronically stored contents of the device.

Wanjiku concedes that no court has ever required a warrant for any border search or seizure. The highest standard that has been applied by the Supreme Court at the border is reasonable suspicion. *Montoya de Hernandez*, 473 U.S. at 541. In that case, border agents detained a woman at the border for approximately sixteen hours because they suspected that she was smuggling illegal drugs in her alimentary canal. Arriving from Bogotá, Colombia, a known source country for narcotics, Montoya de Hernandez had made eight recent trips of short duration to Miami and Los Angeles. On questioning, the agents learned that she spoke no English, had no friends or family in the United States and was carrying $5000 in cash. She traveled with only one small suitcase with a few changes of clothes. Although she claimed to be in the United States to purchase items for her husband's store in Colombia, she had no appointments with merchandise vendors, no hotel reservations, and no plans other than to take taxicabs around Los Angeles to retail stores such as K-Mart and J.C. Penney to buy goods for her husband's store. She could not recall how her plane ticket had been purchased. On the basis of this information, the agents believed that she was a "balloon swallower," and that she was attempting to bring illegal drugs into the country in her alimentary canal. A female customs agent was dispatched to conduct a strip search, which revealed that her abdomen was firm and full. When asked to submit to an x-ray, she at first agreed but then withdrew her consent. The inspector then gave her the option of returning to Colombia on the next flight, agreeing to an x-ray, or remaining in detention until

she produced a monitored bowel movement that would be inspected for balloons or capsules of drugs. 473 U.S. at 532–35.

She chose the first option, but the agents were unsuccessful in finding a flight that evening and she remained in the customs office under observation through the night. At that point, she was given the option of an x-ray or detention pending the monitored bowel movement. She was told that she would have to use a wastebasket in the women's restroom so that agents could examine her stool for balloons. After sixteen hours in detention, she had not defecated or urinated and had refused all food and drink. At that point, customs officials sought a warrant which authorized an x-ray and rectal exam by a physician. The rectal exam led to the discovery of the first of eighty-eight balloons containing a combined total of one half of a kilogram of cocaine. 473 U.S. at 535–36.

The Supreme Court affirmed the denial of her motion to suppress the evidence obtained as a result of her sixteen-hour warrantless detention under these conditions. The Court first noted that the Fourth Amendment commands that searches and seizures be reasonable, and that the permissibility of a particular law enforcement practice is judged by balancing that practice's intrusion on Fourth Amendment interests against its promotion of legitimate government interests. *Montoya de Hernandez*, 473 U.S. at 537. Dating back to the founding era, Congress had granted the Executive plenary authority to conduct searches and seizures at the border without probable cause or a warrant. Because such power is needed to protect the nation, the balancing of interests at the border has been treated very differently than in the interior. 473 U.S. at 537-38. "[N]ot only is the expectation of privacy less at the border than

in the interior, the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border." 473 U.S. at 539-40 (internal citations omitted). *See also Ramsey*, 431 U.S. at 623 n.17 (noting that there are "limited justifiable expectations of privacy at the border" in part because of "the longstanding, constitutionally authorized right of customs officials to search incoming persons and goods"). The Court ultimately held that the detention of a traveler "beyond the scope of a routine customs search and inspection," is justified if the agents "reasonably suspect that the traveler is smuggling contraband in her alimentary canal." 473 U.S. at 541. The Court found that the agents possessed the requisite level of suspicion considering all of the facts known to them regarding this traveler and her trip. 473 U.S. at 542.

The Court later rejected an extension of the requirement of reasonable suspicion at the border for another search that a lower court had characterized as non-routine. *Flores-Montano*, 541 U.S. at 152-53. In that case, border agents had seized thirty-seven kilograms of marijuana from a car entering the United States from Mexico. The drugs were discovered by removing the car's gas tank and disassembling it. The government declined to rely on reasonable suspicion in supporting the search, instead contending that the search was proper as a border search for which no particularized suspicion was required. The Court of Appeals found that the disassembly of the tank was non-routine and required reasonable suspicion, citing *Montoya de Hernandez*. The Supreme Court rejected the comparison:

> The Court of Appeals took the term "routine," fashioned a new balancing test, and extended it to searches of vehicles. But the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person —dignity and privacy interests of the person being searched—simply do not carry over to vehicles. Complex balancing tests to determine what is a "routine" search of a vehicle, as opposed to a more "intrusive" search of a person, have no place in border searches of vehicles.

Flores-Montano, 541 U.S. at 152. Reiterating that the expectation of privacy is less at the border than in the interior, the Court also emphasized that the government's interest in preventing the entry of unwanted persons and effects "is at its zenith at the international border." 541 U.S. at 152, 154. The Court hedged only slightly on the usual rule allowing plenary searches of property at the border, noting that although "it may be true that some searches of property are so destructive as to require a different result, this was not one of them." 541 U.S. at 155–56.

B.

Although our court has yet to confront the precise issue presented here—a non-destructive search of the contents of electronic devices at the border—we have confronted border searches and seizures that we characterized as arguably non-routine and we applied the reasonable suspicion standard to those searches. *Yang*, 286 F.3d at 949 (applying the reasonable

suspicion standard to a search at O'Hare Airport that took place at a different terminal after the traveler had been released from routine inspection at the customs area of the international terminal); *United States v. Johnson*, 991 F.2d 1287, 1291-94 (7th Cir. 1993) (approving a forty-minute seizure of a passenger and the dismantling of her suitcase during an O'Hare Airport border inspection because, even if these actions were "non-routine," customs agents possessed reasonable suspicion to support them). We decided *Johnson* a decade before the Supreme Court rejected the application of the reasonable suspicion standard to the dismantling of a car's gas tank at the border. But in the Seventh Circuit, *Johnson* set the high point at reasonable suspicion for searches that are non-routine. *See also Kaniff v. United States*, 351 F.3d 780, 784-85 (7th Cir. 2003) (finding reasonable suspicion an adequate standard to support a pat down, a partial strip search and a visual body cavity search at the international terminal at O'Hare).

Although conceding that no court has applied a standard higher than reasonable suspicion for even highly intrusive searches at the border, Wanjiku nonetheless argues that the legal landscape for the search of cell phones changed with *Riley* and *Carpenter*. He argues that those cases demonstrate that cell phones present unparalleled privacy interests that require heightened Fourth Amendment protection. Specifically, he asserts that, even in the border context, law enforcement may search cell phones and other electronic devices only with a warrant supported by probable cause. The *Riley* decision preceded the search that was conducted in this case; *Carpenter* was decided three years after the search of Wanjiku's devices. Wanjiku maintains that those decisions require special treat-

ment for the searches of electronic devices in general and cell phones in particular, even at the border.

Turning, then, to those decisions, in *Riley*, the Supreme Court addressed whether police officers could search the contents of a cell phone found in the pocket of an arrestee under the "search incident to the arrest" exception to the warrant requirement of the Fourth Amendment. 573 U.S. at 382. The exception, the Court noted, was rooted in two rationales: the need to protect officer safety, and the interest in preventing the destruction of evidence. 573 U.S. at 383. The exception is limited to personal property "immediately associated with the person of the arrestee." 573 U.S. at 384 (quoting *United States v. Chadwick*, 433 U.S. 1, 15 (1977), abrogated on other grounds by *California v. Acevedo*, 500 U.S. 565 (1991)). In the case of cell phones recovered from the person of the arrestee, the Court concluded that, in the usual case, the data on a cell phone posed no danger to officer safety, *Riley*, 573 U.S. at 387, and there was little likelihood that evidence would be destroyed once the device was secured by law enforcement. 573 U.S. at 389-91.

The Court also addressed the arrestee's reduced privacy expectations upon being taken into police custody, noting that the Fourth Amendment does not fall out of the picture simply because a person has a reduced interest in privacy. 573 U.S. at 392. For example, an arrest in the home does not justify a "top-to-bottom search of a man's house" without a warrant. *Riley*, 573 U.S. at 392 (citing *Chimel v. California*, 395 U.S. 752, 766-67, n.12 (1969)). In assessing the intrusion on privacy implicated in the search of cell phone data, the Court noted:

> 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.

Riley, 573 U.S. at 393. Because of the vast storage capacity of cell phones, the type of data that is collected and stored on these devices, and the pervasiveness of their use:[13]

> a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

---

[13] The Court noted that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley*, 573 U.S. at 385.

573 U.S. at 393–97.[14] In light of these unique characteristics of cell phones, and because a warrantless search of a cell phone found on the person of an arrestee is untethered from the justifications underlying the "search incident to arrest" exception to the warrant requirement, the Court concluded "that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest." 573 U.S. at 401.

In *Carpenter*, the Court assessed whether the government "conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." 138 S. Ct. at 2211. As a person carrying a cell phone moves about throughout the day, radio antennas utilized by wireless carriers collect time-stamped location information each time the phone is in proximity to the antenna site ("cell site"). This data provides an all-encompassing record of the cell phone holder's whereabouts, tracking not only particular movements but potentially revealing familial, political, professional, religious and sexual associations. 138 S. Ct. at 2217. Because cell site data is maintained by wireless carrier companies for up to five years, it also provides a type of information previously unavailable to law enforcement, historical data of where a person was in the past. "[I]ndividuals have a reasonable expectation of privacy in the whole of their physical movements." *Carpenter*, 138 S. Ct. at

---

[14] The Court also addressed the additional complication that not all cell phone data is stored on the device itself, but may be stored in the "cloud," remote servers that serve as extensions of the device's internal memory. *Riley*, 573 U.S. at 397–98. None of the images at issue here were retrieved from cloud storage.

2217. The collection of that data by police, the Court found, therefore constitutes a search, and law enforcement "must generally obtain a warrant supported by probable cause before acquiring such records." 138 S. Ct. at 2221.

Although both of these cases support Wanjiku's general argument that the Supreme Court has recently granted heightened protection to cell phone data, neither case addresses searches at the border where the government's interests are at their zenith, and neither case addresses data stored on other electronic devices such as portable hard drives and laptops.[15] Prior to *Riley*, the Court required nothing more than reasonable suspicion for a highly intrusive border search and seizure wherein a woman was held at the airport for sixteen hours in order for authorities to monitor her next bowel movement. *Montoya de Hernandez*, 473 U.S. at 541. For non-destructive searches of property at the border, the Court required no particularized suspicion at all. *Flores-Montano*, 541 U.S. at 155–56. In *Ramsey*, after noting that border searches, from before the adoption of the Fourth Amendment, have been considered to be reasonable "by the single fact that the person or item in question had entered into our country from out-

---

[15] As we noted above, the first device searched by forensic agents was the portable hard drive, and that search revealed child pornography. At that point, the agents possessed probable cause to search Wanjiku's cell phone. Moreover, the child pornography recovered from Wanjiku's cell phone was not stored on the phone itself but was stored on a micro SD card inserted into the phone, a memory device that was neither password-protected nor encrypted. To the extent that *Riley* gives heightened protection to cell phone data, it is not at all clear that *Riley* would help the defendant here in light of the order in which the agents searched the devices.

side," the Court added that "[t]here has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause." *Ramsey*, 431 U.S. at 619. Moreover, no circuit court, before or after *Riley*, has required more than reasonable suspicion for a border search of cell phones or electronically-stored data. *See United States v. Kolsuz*, 890 F.3d 133, 146–48 (4th Cir. 2018) (finding that some level of particularized suspicion is necessary for a forensic examination of a cell phone at a border but declining to determine whether reasonable suspicion is the appropriate level because the agents reasonably relied on established precedent allowing warrantless border searches of digital devices at the border that are based on at least reasonable suspicion); *United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018) (finding that, at the border, there is "no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property," and noting that, in any case, the agent possessed reasonable suspicion to search the defendant's electronic devices); *United States v. Vergara*, 884 F.3d 1309, 1312 (11th Cir. 2018) (forensic searches of cell phones at the border require neither a warrant nor probable cause; at the border, the highest standard for search is reasonable suspicion); *United States v. Molina-Isidoro*, 884 F.3d 287, 289 (5th Cir. 2018) (declining the defendant's invitation to import *Riley*'s warrant requirement into a border search of a cell phone, where that search was supported by probable cause, and where the agents conducting it acted in good-faith reliance on the longstanding and expansive authority of the government to search persons and their effects at the border without a

warrant, and with at most reasonable suspicion in cases involving highly intrusive searches of a person); *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013) (a comprehensive and intrusive forensic search of a laptop computer (including deleted files in unallocated space) at the border required a showing of reasonable suspicion).

C.

So at the time the agents searched Wanjiku's cell phone, hard drive, and laptop, the Supreme Court required no particularized suspicion for a non-destructive border search of property, and, at most, reasonable suspicion for a highly intrusive border search of a person's most intimate body parts. No court required probable cause and a warrant for a border search of any property, as Wanjiku now asserts. Given the state of the law at the time of these searches of the contents of Wanjiku's electronic devices, the agents therefore possessed an objectively good faith belief that their conduct did not violate the Fourth Amendment because they had reasonable suspicion to conduct the searches. "Courts generally do not suppress unlawfully obtained evidence when the police acted on an objectively good-faith belief that their conduct was lawful at the time of the search." *Velazquez*, 906 F.3d at 560. *See also Davis v. United States*, 564 U.S. 229, 241 (2011) (when binding appellate precedent specifically authorizes a particular police practice, the exclusionary rule should not apply if that precedent is later overruled by the Supreme Court); *United States v. Leon*, 468 U.S. 897, 918–21 (1984) (evidence obtained in objectively good-faith reliance on a subsequently invalidated search warrant should not be excluded); *United States v. Jenkins*, 850 F.3d 912, 918 (7th Cir. 2017) (unlawfully obtained evidence

should not be suppressed when police officers acted with an objectively good-faith belief that their conduct was lawful).

Wanjiku has a two-fold response to the government's assertion of good faith: first, he contends that the government waited too long to raise the good-faith argument. Second, he asserts that the agents did not possess reasonable suspicion at the time they decided to search the contents of his devices, which Agent Toler candidly admitted at the suppression hearing was before Wanjiku even landed at the airport. We take each claim in turn.

1.

The government concedes that it did not raise its good faith claim in the district court but argues that this failure should not be taxed against it. According to the government, it had no reason to argue good faith reliance on reasonable suspicion at the time of briefing in the district court because no court had ever required anything more than reasonable suspicion for any kind of border search. The government also contends that, to the extent that Wanjiku relies on *Carpenter*, the Supreme Court had not yet heard or decided that case at the time of briefing, and this intervening change in law obviates any waiver or forfeiture. Finally, the government contends that, although it may not raise new claims or issues on appeal, we may review new arguments related to preserved claims.

We agree that the government's argument on appeal is simply a new twist on the arguments it preserved below, namely, that the agents acted lawfully because they possessed reasonable suspicion. *See United States v. Billups*, 536 F.3d 574, 578 (7th Cir. 2008) (finding that a "challenge below was

sufficient to preserve [a defendant's] current argument, even if he offers a new twist on that argument based upon additional authority on appeal"). We also agree that we may ignore any waiver or forfeiture because Wanjiku now relies on *Carpenter*, intervening case law. *Velazquez*, 906 F.3d at 560 n.4 (rejecting an argument that the government waited too long to raise good-faith reliance on then-existing precedent when the government raised the issue at its first opportunity following an intervening change in the law). Indeed, in the district court, Wanjiku argued primarily that reasonable suspicion was needed to support the search, which would not have alerted the government to the need to argue good-faith reliance on existing precedent on the warrant issue. As we noted above, in his reply brief on the Motion to Suppress, Wanjiku argued that "a reasonable suspicion standard should apply, but also … in the wake of *Riley v. California*, 134 S. Ct. 2473 (2014), *there are grounds for a higher standard,* namely probable cause and a warrant." R. 50, at 1 (emphasis added). During oral argument at the suppression hearing, he argued for a "heightened standard" but conceded that the law was unsettled, and contended that there was no guiding precedent for electronic border searches in this circuit. He did not press the argument he makes now, that although this is an issue of first impression in the Seventh Circuit, *Riley* and *Carpenter* unequivocally require probable cause and a warrant. Instead, he argued below that the standard *should* be probable cause and a warrant, not that it already was:

> So we believe that a heightened standard should apply. I know it may be just for preservation purposes that we believe that standard should

> be probable cause and a warrant. But, at a minimum, that there should be reasonable suspicion.

R. 59, Tr. at 127. The government rightly responded to the argument that Wanjiku actually presented: that the reasonable suspicion standard applied, and that no court had required probable cause and a warrant. Now that Wanjiku shifts his focus and raises as his primary argument on appeal that the search required probable cause and a warrant, the government may argue that the agents reasonably relied on the well-established case law supporting the lesser standard of reasonable suspicion.

2.

We turn to Wanjiku's contention that the court should measure reasonable suspicion at the moment that the agents decided to search his devices. Agent Toler conceded that he had decided to search the contents of Wanjiku's devices before he landed at the airport. But the subjective beliefs or intentions of law enforcement officers are irrelevant in determining whether reasonable suspicion to search existed. *United States v. Patton*, 705 F.3d 734, 738 (7th Cir. 2013) (reasonable suspicion is an objective standard and an officer's subjective intention to frisk a person from the outset of the encounter is irrelevant to that objective assessment). *See also Whren v. United States*, 517 U.S. 806, 813 (1996) ("Subjective intentions play no role in ordinary, probable-cause Fourth Amendment analysis."); *Terry v. Ohio*, 392 U.S. 1, 21–22 (1968) (courts evaluate the reasonableness of a particular search or seizure in light of the particular circumstances judged against an objective standard). That objective test is applied to "the facts available to the officer *at*

the moment of the seizure or the search," and asks whether those facts would warrant a person of reasonable caution in the belief that the action taken was appropriate. *Terry*, 362 U.S. at 21–22 (emphasis added). Thus, we must measure whether reasonable suspicion existed at the moment of the search of Wanjiku's devices, not at the time the agents decided to conduct the search.

3.

The district court found that, at the time the agents actually conducted the searches of Wanjiku's electronic devices, they knew:

> 1) that Mr. Wanjiku was a U.S. citizen male in his 40's returning from an extended trip by himself to the Philippines, a country with which he had no obvious connection, to which he had traveled several times in the preceding two years, and which was a known destination for sex tourism; 2) that Mr. Wanjiku had been arrested for contributing to the delinquency of a minor, a crime that, like child pornography, involved a minor victim; 3) that Mr. Wanjiku used an email address that Officer Toler construed as a possible reference to male genitalia; 4) that Mr. Wanjiku's Facebook page included a profile picture of him in a mask and showed that he had multiple friends who seemed very young; 5) that the primary border officer's notes stated that Mr. Wanjiku had been "evasive for questioning" during primary inspection; 5) that

> Mr. Wanjiku left the secondary inspection line prior to his inspection—something Officer Toler stated he had never seen before—and offered a questionable explanation for his departure after being escorted back to the line by an ICE agent; and 6) that Mr. Wanjiku appeared visibly nervous during inspection, sweating profusely and shifting his weight.
>
> In addition, upon examining the contents of Mr. Wanjiku's bag, Officer Toler found hotel receipts that called into question his previous account of where he had stayed during his trip. Officer Toler also found condoms, syringes, and injectable testosterone.

United States v. Wanjiku, 2017 WL 1304087, *6 (N.D. Ill. April 6, 2017).[16]

We agree with the district court that these facts "raised a reasonable suspicion that a search of Mr. Wanjiku's electronic devices would reveal evidence of criminal activity involving minors." *Id*. *See also Terry*, 362 U.S. at 27 ("in determining whether the officer acted reasonably in such circumstances,

---

[16] We take a moment to note a fact on which the district court apparently did **not** rely in assessing reasonable suspicion. The court did not mention the images of Wanjiku with a male of unknown age that Agent Toler saw when he directed Wanjiku to unlock his phone so that the agent could manually scroll through the photos. Although Wanjiku also contests this manual, non-forensic search of his phone, that search occurred at a time when Agent Toler already possessed all of the facts that gave rise to reasonable suspicion.

due weight must be given, not to his inchoate and unparticularized suspicion or 'hunch,' but to the specific reasonable inferences which he is entitled to draw from the facts in light of his experience."). Reasonable suspicion is a "commonsense, nontechnical" concept that deals with "the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Ornelas v. United States*, 517 U.S. 690, 695 (1996) (quoting *Illinois v. Gates*, 462 U.S. 213, 231 (1983)). Although, as Wanjiku asserts, there may be innocent explanations for some of the facts on which the officers relied, "reasonable suspicion 'need not rule out the possibility of innocent conduct.'" *Navarette v. California*, 572 U.S. 393, 403 (2014) (quoting *United States v. Arvizu*, 534 U.S. 266, 277 (2002)). In light of the facts known to the agents at the time they conducted the searches of Wanjiku's electronic devices, the agents possessed "a particularized and objective basis" for suspecting that Wanjiku was engaged in criminal activity. *Ornelas*, 517 U.S. at 696. *See also Yang*, 286 F.3d at 949 (providing a non-exhaustive list of illustrative factors giving rise to reasonable suspicion in a border search including nervous or unusual conduct, tips from informants, travel itinerary, discovery of incriminating matter during routine searches, information from a search or interrogation of a traveling companion, and evasive or contradictory answers).

III.

In sum, the agents possessed reasonable suspicion to search Wanjiku's electronic devices, including his cell phone, portable hard drive, and laptop computer. At the time that they conducted these searches, they reasonably relied on Supreme Court precedent that required no suspicion for non-destructive

border searches of property, and nothing more than reasonable suspicion for highly intrusive border searches of persons. The Court had also indicated that probable cause and a warrant had never been required for any border search. We therefore need not reach the issue of what level of suspicion is required (if any) for searches of electronic devices at the border, and reserve that question for a case in which it matters to the outcome. The district court committed no error in declining to suppress the electronic evidence that formed the basis of Wanjiku's conviction.

AFFIRMED.