[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 17-11561

D.C. Docket No. 1:15-cr-00045-MHC-JKL-1

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

KARL TOUSET,

Defendant-Appellant.

Appeal from the United States District Court
for the Northern District of Georgia

(May 23, 2018)

Before WILLIAM PRYOR and JULIE CARNES, Circuit Judges, and CORRIGAN,[*] District Judge.

WILLIAM PRYOR, Circuit Judge:

[*] Honorable Timothy J. Corrigan, United States District Judge for the Middle District of Florida, sitting by designation.

This appeal presents the question whether the Fourth Amendment requires reasonable suspicion for a forensic search of an electronic device at the border. U.S. Const. amend. IV. Karl Touset appeals the denial of his motions to suppress the child pornography found on electronic devices that he carried with him when he entered the country and the fruit of later searches. We recently held that the Fourth Amendment does not require a warrant or probable cause for a forensic search of a cell phone at the border. *United States v. Vergara*, 884 F.3d 1309 (11th Cir. 2018). Touset argues that, in the light of the decision of the Supreme Court in *Riley v. California*, 134 S. Ct. 2473 (2014), reasonable suspicion was required for the forensic searches of his electronic devices. But our precedents about border searches of property make clear that no suspicion is necessary to search electronic devices at the border. Alternatively, the border agents had reasonable suspicion to search Touset's electronic devices. We affirm.

I. BACKGROUND

After a series of investigations by private organizations and the government suggested that Karl Touset was involved with child pornography, border agents forensically searched his electronic devices after he arrived at the Atlanta airport on an international flight. Xoom, a company that transmits money, identified several people it suspected were involved with child pornography based on a pattern of "frequent low money transfers to" individuals in "source countries for

sex tourism and child pornography," including the Philippines. Xoom alerted the National Center for Missing and Exploited Children and notified Yahoo because some of the people it suspected were involved with child pornography used Yahoo email and messenger accounts.

Yahoo then conducted its own investigation into the accounts identified by Xoom and found a file with child pornography in the account for the email address iloveyousomuch0820@yahoo.com. This email account listed a phone number in the Philippines. Yahoo then sent tips to the National Center, which notified the Cyber Crime Center of the Department of Homeland Security.

While performing its own investigation, the Cyber Center subpoenaed transaction data related to the iloveyousomuch0820@yahoo.com email account and the Philippine phone number associated with it from several companies that transmit money. One of those companies, Western Union, provided information about an account associated with the Philippine phone number. The information established that an account that listed Touset's name and a post office box in Marietta, Georgia, had sent three payments to the account associated with the Philippine phone number. In March 2013, the account associated with Touset sent a payment of $35 to the account associated with the Philippine phone number; in April 2013, it sent another payment of $35; and in July 2013, it sent a payment of $37. Based on this information, the Department placed a "look-out" on Touset so

that his luggage and electronic devices would be searched when he returned to the country.

After Touset arrived on an international flight at the airport in Atlanta, Georgia, on December 21, 2014, Derek Escobar, an officer of the Customs and Border Protection Agency, inspected Touset's luggage. Touset had two iPhones, a camera, two laptops, two external hard drives, and two tablets. Escobar manually inspected the iPhones and the camera, found no child pornography, and returned those devices to Touset. But the Agency detained the remaining electronic devices, and computer forensic analysts at the Department later searched them. Forensic searches revealed child pornography on the two laptops and the two external hard drives.

Based on that information, Dianna Ford, a special agent of the Department, obtained a warrant to search Touset's home in Marietta, Georgia. Ford and about 14 other agents executed the warrant on January 28, 2015. During the execution of the warrant, Ford and another agent read Touset his rights under *Miranda v. Arizona*, 384 U.S. 436 (1966), and recorded an interview with him. Ford arrested Touset after that interview.

Evidence obtained by the government established that Touset purchased thousands of images of child pornography. Over the course of several years, Touset sent more than $55,000 to the Philippines for pornographic pictures, videos,

and webcam sessions. In some webcam sessions, he instructed prepubescent girls to display and manipulate their genitals. Touset also created an Excel spreadsheet that documented the names, ages, and birthdates of those young girls as well as his notes about them.

A grand jury indicted Touset on three counts: knowingly receiving child pornography, 18 U.S.C. § 2252(a)(2) & (b)(1); knowingly transporting and shipping child pornography, 18 U.S.C. § 2252(a)(1) & (b)(1); and knowingly possessing a computer and computer-storage device containing child pornography, 18 U.S.C. § 2252(a)(4)(B) & (b)(2). Touset initially pleaded not guilty to the charges.

Touset filed motions to suppress the evidence obtained from his electronic devices at the border, as well as the fruit of those searches. After an evidentiary hearing at which Escobar and Ford testified, the magistrate judge recommended denying Touset's motions to suppress. The magistrate judge explained that the parties agreed that the government "needed reasonable suspicion of criminal activity in order to lawfully detain for further analysis and search [Touset's] electronic devices." The magistrate judge found that reasonable suspicion was present because "[t]he collective information of the officers allowed the reasonable inference that Touset had made three small payments through Western Union to an entity in the Philippines, a country known for child exploitation," and that entity

"used an email address that had previously received or sent child pornography." And the magistrate judge rejected Touset's argument that, because his most recent payment to the Western Union account associated with the Philippine phone number occurred about one and a half years before his electronic devices were searched, that evidence was stale. Instead, the magistrate judge found that the evidence of Touset's payments was not stale because "[f]iles on a computer are less likely than other types of contraband to disappear over time and can often be recovered even if they are deleted."

The district court adopted the magistrate judge's report and recommendation over Touset's objections. The district court relied on the decision of the Ninth Circuit in *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013) (en banc), and concluded that reasonable suspicion is required for a forensic search of electronic devices at the border. The district court found that reasonable suspicion existed for the detention and forensic search of Touset's electronic devices. And the district court agreed with the magistrate judge that the evidence was not stale.

Touset pleaded guilty to knowingly transporting child pornography, but reserved his right to appeal the denial of his motion to suppress. The government dismissed the other two counts. And the district court sentenced Touset to 120 months of imprisonment and supervision for life.

II. STANDARD OF REVIEW

"Because rulings on motions to suppress involve mixed questions of fact and law, we review the district court's factual findings for clear error, and its application of the law to the facts *de novo*." *United States v. Ransfer*, 749 F.3d 914, 921 (11th Cir. 2014) (quoting *United States v. Bervaldi*, 226 F.3d 1256, 1262 (11th Cir. 2000)). We construe "all facts . . . in the light most favorable to the prevailing party below." *Id.* (quoting *Bervaldi*, 226 F.3d at 1262). And "[t]he individual challenging the search bears the burdens of proof and persuasion." *United States v. Newsome*, 475 F.3d 1221, 1224 (11th Cir. 2007) (citation and internal quotation marks omitted).

III. DISCUSSION

We divide our discussion in two parts. First, we explain that the Fourth Amendment does not require any suspicion for forensic searches of electronic devices at the border. Second, we explain that, in the alternative, the searches of Touset's electronic devices were supported by reasonable suspicion.

A. The Fourth Amendment Permits Forensic Searches of Electronic Devices at the Border Without Suspicion.

The Fourth Amendment to the Constitution provides, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ." U.S. Const. amend. IV. Ordinarily,

"reasonableness requires the obtaining of a judicial warrant." *United States v. Vergara*, 884 F.3d 1309, 1312 (11th Cir. 2018) (alteration adopted) (quoting *Riley v. California*, 134 S. Ct. 2473, 2482 (2014)). But border searches are different. *Id.*

As we recently reiterated, searches at the border of the country "'never' require probable cause or a warrant." *Id.* (quoting *United States v. Ramsey*, 431 U.S. 606, 619 (1977)). The First Congress—the same one that proposed the Fourth Amendment—empowered customs officials to stop and search without a warrant any vessel or cargo suspected of illegally entering our nation. *See* Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43 (1789); *Ramsey*, 431 U.S. at 616–17 ("The historical importance of the enactment of this customs statute by the same Congress which proposed the Fourth Amendment is, we think, manifest."); *Boyd v. United States*, 116 U.S. 616, 623 (1886) ("[I]t is clear that the members of that body did not regard searches and seizures of [contraband] as 'unreasonable,' and they are not embraced within the prohibition of the [Fourth] [A]mendment."). And a year later, Congress expanded that power by permitting customs officials to board vessels even before they reached the United States. *See* Act of Aug. 4, 1790, ch. 35, § 31, 1 Stat. 145, 164–65 (1790); *United States v. Villamonte-Marquez*, 462 U.S. 579, 584 (1983).

"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." *United States v. 12 200-Ft. Reels of Super 8MM. Film*, 413 U.S. 123, 125 (1973). Congress has "broad powers . . . to prevent smuggling and to prevent prohibited articles from entry," *id.*, under its plenary authority "[t]o lay and collect Taxes, Duties, Imposts and Excises," U.S. Const. art. I, § 8, cl. 1, "[t]o regulate Commerce with foreign Nations," *id.* art. I, § 8, cl. 3, and "[t]o establish a[] uniform Rule of Naturalization," *id.* art. I, § 8, cl. 4. And because child pornography is unprotected by the First Amendment, "Congress may declare it contraband and prohibit its importation." *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376–77 (1971) (plurality opinion); *accord 12 200-Ft. Reels*, 413 U.S. at 128–29; *see also Osborne v. Ohio*, 495 U.S. 103, 111 (1990) ("[W]e cannot fault [the government] for attempting to stamp out [child pornography] at all levels in the distribution chain.").

Ordinarily, searches at the border are reasonable without suspicion "simply by virtue of the fact that they occur at the border." *United States v. Alfaro-Moncada*, 607 F.3d 720, 728 (11th Cir. 2010) (quoting *Denson v. United States*, 574 F.3d 1318, 1339 (11th Cir. 2009)). The Supreme Court has held that it is reasonable to conduct without suspicion "[r]outine searches of the persons and effects of entrants" at our borders. *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). And we have similarly explained that, at the border, routine "pat-down search[es] or frisk[s]" and searches of "[a] traveler's luggage,"

"[i]ncoming international mail," and "[v]ehicles" are all reasonable "without any level of suspicion." *Alfaro-Moncada*, 607 F.3d at 728 (collecting cases). A traveler's "right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during . . . a search." *Thirty-Seven Photographs*, 402 U.S. at 376 (plurality opinion).

The Supreme Court has never required reasonable suspicion for a search of property at the border, however non-routine and intrusive, and neither have we. Although in one decision the Supreme Court required reasonable suspicion for the prolonged detention of a *person* until she excreted the contraband that she was suspected of "smuggling . . . in her alimentary canal" or submitted to an x-ray or rectal examination, *Montoya de Hernandez*, 473 U.S. at 541; *see also id.* at 534–35, it has never applied this requirement to property. Nor has it "been willing to distinguish . . . between different types of property." *Cotterman*, 709 F.3d at 975 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment). Indeed, it held in *United States v. Flores-Montano* that the government may "remove, disassemble, and reassemble a vehicle's fuel tank" at the border without any suspicion. 541 U.S. 149, 155 (2004). It explained that "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." *Id*. at 152. And it rejected a judicial attempt to distinguish between "routine" and "nonroutine" searches and to craft "[c]omplex balancing tests to determine what [constitutes] a 'routine' search of a vehicle, as opposed to a more 'intrusive' search of a person." *Id.* We have been similarly unwilling to distinguish between different kinds of property. For example, we have upheld "a search without reasonable suspicion of a crew member's living quarters on a foreign cargo vessel that [wa]s entering this country," *Alfaro-Moncada*, 607 F.3d at 727, even though "[a] cabin is a crew member's home—and a home 'receives the greatest Fourth Amendment protection,'" *id.* at 729 (quoting *United States v. McGough*, 412 F.3d 1232, 1236 (11th Cir. 2005)); *accord id.* at 732.

We see 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. Just as the United States is entitled to search a fuel tank for drugs, *see Flores-Montano*, 541 U.S. at 155, it is entitled to search a flash drive for child pornography. And it does not make sense to say that electronic devices should receive special treatment because so many people now own them or because they can store vast quantities of records or effects. The same could be said for a recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents. Border agents bear the same responsibility for preventing the

importation of contraband in a traveler's possession regardless of advances in technology. Indeed, inspection of a traveler's property at the border "is an old practice and is intimately associated with excluding illegal articles from the country." *Thirty-Seven Photographs*, 402 U.S. at 376 (plurality opinion).

In contrast with searches of property, we have required reasonable suspicion at the border only "for highly intrusive searches of a person's body." *Alfaro-Moncada*, 607 F.3d at 729. Even though the Supreme Court has declined to decide "what level of suspicion, if any, is required for [such] nonroutine border searches [of a person]," *Montoya de Hernandez*, 473 U.S. at 541 n.4, we have required reasonable suspicion for "a strip search or an x-ray examination," *Alfaro-Moncada*, 607 F.3d at 729. We have defined the "intrusiveness" of a search of a person's body that requires reasonable suspicion "in terms of the indignity that will be suffered by the person being searched," in contrast with "whether one search will reveal more than another." *United States v. Vega-Barvo*, 729 F.2d 1341, 1345 (11th Cir. 1984); *accord id.* at 1346. And "we have isolated three factors which contribute to the personal indignity endured by the person searched: (1) physical contact between the searcher and the person searched; (2) exposure of intimate body parts; and (3) use of force." *Id.* at 1346.

These factors are irrelevant to searches of electronic devices. A forensic search of an electronic device is not like a strip search or an x-ray; it does not

require border agents to touch a traveler's body, to expose intimate body parts, or to use any physical force against him. Although it may intrude on the privacy of the owner, a forensic search of an electronic device is a search of property. And our precedents do not require suspicion for intrusive searches of any property at the border. *See Alfaro-Moncada*, 607 F.3d at 728–29, 732.

To be sure, the Fourth and the Ninth Circuits have concluded—in divided decisions—that the Fourth Amendment requires at least reasonable suspicion for forensic searches of electronic devices at the border. *United States v. Kolsuz*, 890 F.3d 133, 144 (4th Cir. 2018); *Cotterman*, 709 F.3d at 968. In *Cotterman*, the Ninth Circuit equated a forensic search to "a computer strip search," 709 F.3d at 966, and stated that "[s]uch a thorough and detailed search of the most intimate details of one's life is a substantial intrusion upon personal privacy and dignity," *id.* at 968. And it reasoned that "[i]ntrusiveness includes both the extent of a search as well as the degree of indignity that may accompany a search." *Id.* at 967 (quoting *United States v. Ramos-Saenz*, 36 F.3d 59, 61 n.3 (9th Cir. 1994)). The Fourth Circuit later explained that the intervening decision of the Supreme Court in *Riley* "confirmed" that reasoning. *Kolsuz*, 890 F.3d at 145. And it revived the distinction between routine and nonroutine searches of property, *see id.* at 144–47, that the Supreme Court rejected in *Flores-Montano*, 541 U.S. at 152.

We are unpersuaded. Although the Supreme Court stressed in *Riley* that the search of a cell phone risks a significant intrusion on privacy, our decision in *Vergara* made clear that *Riley*, which involved the search-incident-to-arrest exception, does not apply to searches at the border. 884 F.3d at 1312 ("[T]he Supreme Court expressly limited its holding to the search-incident-to-arrest exception."). And our precedent considers only the "personal indignity" of a search, not its extensiveness. *Vega-Barvo*, 729 F.2d at 1346. Again, we fail to see how the personal nature of data stored on electronic devices could trigger this kind of indignity when our precedent establishes that a suspicionless search of a home at the border does not. *See Alfaro-Moncada*, 607 F.3d at 729, 732. Property and persons are different. *See Flores-Montano*, 541 U.S. at 152.

We are also unpersuaded that a traveler's privacy interest should be given greater weight than the "paramount interest [of the sovereign] in protecting . . . its territorial integrity." *Id.* at 153. The Ninth and Fourth Circuits stressed the former interest and asserted that travelers have no practical options to protect their privacy when traveling abroad. For example, the Ninth Circuit explained that it is "impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel" and that "removing files unnecessary to an impending trip" is "a time-consuming task that may not even effectively erase the files." *Cotterman*,

709 F.3d at 965. The Fourth Circuit added that "it is neither 'realistic nor reasonable to expect the average traveler to leave his digital devices at home when traveling.'" *Kolsuz*, 890 F.3d at 145 (quoting *United States v. Saboonchi*, 990 F. Supp. 2d 536, 556 (D. Md. 2014)). But a traveler's "expectation of privacy is less at the border," *Flores-Montano*, 541 U.S. at 154, and the Fourth Amendment does not guarantee the right to travel without great inconvenience, even within our borders, *see Corbett v. Transp. Sec. Admin.*, 767 F.3d 1171, 1179 (11th Cir. 2014) (holding that airport screening "is a reasonable administrative search under the Fourth Amendment"); *see also Kolsuz*, 890 F.3d at 152 (Wilkinson, J., concurring in the judgment) ("Our new world has brought inconvenience and intrusions on an indiscriminate basis, which none of us welcome, but which most of us undergo in the interest of assuring a larger common good."). Anyone who has recently taken a domestic flight likely experienced inconvenient screening procedures that require passengers to unpack electronic devices, separate and limit liquids, gels, and creams, remove their shoes, and walk through a full-body scanner. *See Corbett*, 767 F.3d at 1174 (explaining that a traveler must walk through a scanner or undergo a pat-down in airports). Travelers "crossing a border . . . [are] on notice that a search may be made," *Alfaro-Moncada*, 607 F.3d at 732 (quoting *United States v. Hidalgo-Gato*, 703 F.2d 1267, 1271 (11th Cir. 1983)), and they are free to leave any property they do not want searched—unlike their bodies—at home.

In contrast with the diminished privacy interests of travelers, "[t]he [g]overnment's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *Flores-Montano*, 541 U.S. at 152. As we have explained, child pornography, no less than drugs or other kinds of contraband, is prohibited from "enter[ing] the country," *Ramsey*, 431 U.S. at 620, and the government interest in stopping contraband at the border does not depend on whether child pornography takes the form of digital files or physical photographs.

Nothing in *Riley* undermines this interest. In *Riley*, the Supreme Court explained that the rationales that support the search-incident-to-arrest exception—namely the concerns of "harm to officers and destruction of evidence"—did not "ha[ve] much force with respect to digital content on cell phones," 134 S. Ct. at 2484, because "digital data" does not pose "comparable risks," *id.* at 2485. But "digital" child pornography poses the same exact "risk" of unlawful entry at the border as its physical counterpart. If anything, the advent of sophisticated technological means for concealing contraband only heightens the need of the government to search property at the border unencumbered by judicial second-guessing.

Indeed, if we were to require reasonable suspicion for searches of electronic devices, we would create special protection for the property most often used to store and disseminate child pornography. With the advent of the internet, child

pornography offenses overwhelmingly involve the use of electronic devices for the receipt, storage, and distribution of unlawful images. *See* U.S. Sent'g Comm'n, *Federal Child Pornography Offenses* 5, 71 (2012); *see also United States v. Williams*, 553 U.S. 285, 307 (2008) ("Both the State and Federal Governments have sought to suppress [child pornography] for many years, only to find it proliferating through the new medium of the Internet."). And law enforcement officers routinely investigate child-pornography offenses by forensically searching an individual's electronic devices. *See* U.S. Sent'g Comm'n, *supra*, at 67–71. We see no reason why we would permit traditional, invasive searches of all other kinds of property, *see Alfaro-Moncada*, 607 F.3d at 724–25, 728, 732, but create a special rule that will benefit offenders who now conceal contraband in a new kind of property.

After all, our nation has classified child pornography as contraband for good reason. The possession of child pornography "harms and debases the most defenseless of our citizens," *Williams*, 553 U.S. at 307, in profound and lasting ways. The harm that victims suffer during the production of child pornography "is exacerbated by the[] circulation" of "a permanent record of the child['s] participation." *New York v. Ferber*, 458 U.S. 747, 759 (1982); *see also* U.S. Sent'g Comm'n, *supra*, at 118. Victims know that countless people may obtain their images, *see United States v. Pugh*, 515 F.3d 1179, 1196 (11th Cir. 2008), and use

them for sexual gratification, *see* U.S. Sent'g Comm'n, *supra*, at 113, 118. Victims also know that their images may contribute to the abuse of new victims. *See id.* The online promotion and sharing of child pornography validates the sexual exploitation of children and "may incite or encourage others to sexually abuse children." *United States v. Irey*, 612 F.3d 1160, 1208 (11th Cir. 2010) (en banc); *see also* U.S. Sent'g Comm'n, *supra*, at 312. And there is evidence that offenders use child pornography to convince children to participate in their abuse. U.S. Sent'g Comm'n, *supra*, at 312. Consumers of child pornography who "'merely' or 'passively' receive or possess child pornography directly contribute to this continuing victimization." *Pugh*, 515 F.3d at 1196 (quoting *United States v. Goff*, 501 F.3d 250, 259 (3d Cir. 2007)). And "[t]he greater the customer demand for child pornography, the more that will be produced." *Irey*, 612 F.3d at 1212 (quoting *United States v. Goldberg*, 491 F.3d 668, 672 (7th Cir. 2007)). We should not invent heightened constitutional protection for travelers who cross our borders with this contraband in tow.

Of course, nothing prevents Congress from enacting laws that provide greater protections than the Fourth Amendment requires. Indeed, Congress has repeatedly exercised this power "to strike a balance between privacy and security in the context of digital searches." *Kolsuz*, 890 F.3d at 150 (Wilkinson, J., concurring in the judgment) (citing USA Freedom Act of 2015, Pub. L. No. 114-

23, 129 Stat. 268; Wiretap Act, Pub. L. No. 90-351, 82 Stat. 197 (1961), *amended by* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, *and* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 18 U.S.C. §§ 2510–2522 (2012)); Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 Mich. L. Rev. 1117, 1120 (2017)). The First Congress required officers to have "reason to suspect" the concealment of "goods, wares or merchandise subject to duty" before the officers could "enter any ship or vessel" "to search for, seize, and secure any such goods, wares or merchandise." Act of July 31, 1789, ch. 5, § 24, 1 Stat. at 43. More recently, Congress enacted special protections for financial records in the Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, tit. XI, 92 Stat. 3641, 3697 (codified at 12 U.S.C. § 3408), and for cell tower location information in the Stored Communications Act, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860 (1986) (codified at 18 U.S.C. §§ 2701–2712;); *see also United States v. Davis*, 785 F.3d 498, 519 (11th Cir. 2015) (en banc) (W. Pryor, J., concurring) (explaining that the Stored Communications Act provides "additional protections" for that information).

Instead of "charging unnecessarily ahead," we must allow Congress to design the appropriate standard "through the more adaptable legislative process and the wider lens of legislative hearings." *Kolsuz*, 890 F.3d at 150 (Wilkinson, J.,

concurring in the judgment). Such a "legislative process would be informed by numerous representatives of the executive branch, who can lend their practical insights and experience to the inquiry." *Id.* at 151. "The dangers of judicial standard-setting in an area as sensitive as border searches [are] . . . apparent." *Id.* "Simply put, we must apply the law and leave the task of developing new rules for rapidly changing technologies to the branch most capable of weighing the costs and benefits of doing so." *Davis*, 785 F.3d at 520 (W. Pryor, J., concurring). Judicial restraint is especially important in the context of border searches, "where there is a longstanding historical practice . . . of deferring to the legislative and executive branches." *Kolsuz*, 890 F.3d at 153 (Wilkinson, J., concurring in the judgment).

B. In the Alternative, Reasonable Suspicion Existed for the Forensic Searches of Touset's Electronic Devices.

Alternatively, the district court correctly denied Touset's motions to suppress because the forensic searches of his electronic devices were supported by reasonable suspicion. Touset argues that the government lacked reasonable suspicion because the evidence that he sent three separate payments to the Western Union account associated with a Philippine phone number was stale and because the evidence did not show that he had possessed child pornography or would possess it on his electronic devices. We disagree.

"Reasonable suspicion . . . must be based upon a 'particularized and objective basis for suspecting the particular person of criminal activity.'" *Denson*, 574 F.3d at 1341 (alteration adopted) (quoting *United States v. Cortez*, 449 U.S. 411, 417–18 (1981)). The "inquiry focuses on the information available to the officers at the time of the stop." *United States v. Lewis*, 674 F.3d 1298, 1305 (11th Cir. 2012).

The government had a "particularized and objective basis for suspecting" that Touset possessed child pornography on his electronic devices. *Denson*, 574 F.3d at 1341 (citation and internal quotation marks omitted). The government knew that Touset had sent three low-money transfers of $35, $35, and $37 to a Western Union account; that the Western Union account was associated with a Philippine phone number that was associated with the email account of iloveyousomuch0820@yahoo.com; that the email account had contained an image of child pornography; that the Philippines was a source country for child pornography; that a pattern of "frequent low money transfers" is associated with child pornography; and that Touset was traveling with nine electronic devices. Together, this evidence provided reasonable suspicion for the forensic searches of Touset's electronic devices.

The "staleness doctrine . . . requires that the information supporting the government's application for a warrant must show that probable cause exists at the

time the warrant issues." *Bervaldi*, 226 F.3d at 1264. And the staleness doctrine also applies to reasonable suspicion. *Id.* at 1264–65; *see also United States v. Carter*, 566 F.3d 970, 975 (11th Cir. 2009). "[S]taleness is an issue that courts must decide by evaluating the facts of a particular case . . . ." *United States v. Domme*, 753 F.2d 950, 953 (11th Cir. 1985). Courts consider "the length of time" as well as "the nature of the suspected crime (discrete crimes or ongoing conspiracy), habits of the accused, character of the items sought, and nature and function of the premises to be searched." *Bervaldi*, 226 F.3d at 1265 (citation and internal quotation marks omitted). We have explained that "[t]here is no particular rule or time limit for when information becomes stale." *Id.*

Our sister circuits have repeatedly rejected staleness challenges in appeals involving child pornography. They have observed that "pedophiles rarely, if ever, dispose of child pornography." *United States v. Zimmerman*, 277 F.3d 426, 434 (3d Cir. 2002); *see also United States v. Burkhart*, 602 F.3d 1202, 1206–07 (10th Cir. 2010); *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008); *United States v. Hay*, 231 F.3d 630, 636 (9th Cir. 2000). And probable cause of involvement in *electronic* child pornography remains even longer because deleted files can remain on electronic devices. *See United States v. Frechette*, 583 F.3d 374, 379 (6th Cir. 2009); *Hay*, 231 F.3d at 636. As the Tenth Circuit explained, "information that a person received electronic images of child pornography is less

likely than information about drugs, for example, to go stale because the electronic images are not subject to spoilage or consumption." *Burkhart*, 602 F.3d at 1207. And other circuits have ruled that probable cause remained after passages of time similar to the interval here. *See, e.g.*, *Frechette*, 583 F.3d at 378–79 (16 months); *Morales-Aldahondo*, 524 F.3d at 119 (three years).

We are persuaded that the reasoning of our sister circuits applies in this circumstance. The evidence that Touset made three separate payments to the Western Union account associated with the Philippine phone number was not stale about a year and a half later. That evidence suggested that Touset likely received child pornography electronically and had child pornography stored on his electronic devices.

IV. CONCLUSION

We **AFFIRM** Touset's judgment of conviction and sentence.

CORRIGAN, District Judge, concurring in part and concurring in the judgment:

I concur in the majority opinion, except as to Part III.A. As the Court notes, the Fourth and Ninth Circuits have concluded that the Fourth Amendment requires at least reasonable suspicion for forensic searches of electronic devices at the border. *See* Maj. Op. at 13, citing *United States v. Kolsuz*, __ F.3d __, No. 16-4687, slip op. at 19 (4th Cir. May 9, 2018), and *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013). In the district court, the government agreed that the applicable Fourth Amendment test was whether there was reasonable suspicion of criminal activity such that border agents could detain Touset's electronic devices for forensic analysis. The district court found reasonable suspicion and upheld the search.

However, on appeal, the government goes beyond its position in the district court and argues that border agents need no justification whatsoever to detain (in this case for seventeen days) and forensically search electronic devices of any American citizen returning from abroad. This new-found government position presents a different and difficult question, one not addressed by the Supreme Court or (until today) any appellate court. In my view, this Court need not reach this issue to decide this case. I therefore concur only in the Court's alternative holding that "the district court correctly denied Touset's motions to suppress because the

forensic searches of his electronic devices were supported by reasonable suspicion." Maj. Op. at 21.