RECENT CASES

FOURTH AMENDMENT — BORDER SEARCH EXCEPTION — FIRST CIRCUIT UPHOLDS WARRANTLESS, SUSPICIONLESS SEARCHES OF ELECTRONIC DEVICES AT THE BORDER. — *Alasaad v. Mayorkas*, 988 F.3d 8 (1st Cir. 2021).

Electronic-device searches at the border[1] have increased sharply in recent years.[2] Such searches require neither a warrant nor probable cause due to the long-recognized exemption of routine border searches from the Fourth Amendment's traditional requirements.[3] The Supreme Court has not yet considered the application of the border search exception to electronic devices,[4] and lower courts have split over the level of suspicion required for certain device searches.[5] Recently, in *Alasaad v. Mayorkas*,[6] the First Circuit upheld the constitutionality of performing "basic"[7] device searches at the border without suspicion and created another circuit split by broadening the scope of the border search exception beyond the interdiction of contraband.[8] In doing so, the court not only

---

[1] The "border" includes the physical border and its functional equivalents, including airports. Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973).

[2] In fiscal year 2019, U.S. Customs and Border Protection (CBP) searched 40,913 electronic devices at the border, *CBP Statement on Border Search of Electronic Devices*, U.S. CUSTOMS & BORDER PROT. (Oct. 30, 2019), https://www.cbp.gov/newsroom/speeches-and-statements/cbp-statement-border-search-electronic-devices [https://perma.cc/MG56-3VGL], compared to 8,503 devices only four years prior, Laura K. Donohue, *Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches*, 128 YALE L.J.F. 961, 961 (2019).

[3] *See* United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) ("Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country.").

[4] Rebecca M. Rowland, Note, *Border Searches of Electronic Devices*, 97 WASH. U. L. REV. 545, 546 (2019).

[5] *Compare* United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (holding that forensic search of a laptop requires reasonable suspicion), *and* United States v. Kolsuz, 890 F.3d 133, 146 (4th Cir. 2018) (holding that forensic search of a cell phone requires "some form of individualized suspicion"), *with* United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018) (upholding suspicionless forensic searches of electronic devices). Forensic searches involve the use of forensic software that can be used "to access all active or readable files on the device, as well as password-protected data, hidden or encrypted data, deleted files, metadata, and unallocated file space." Rowland, *supra* note 4, at 545–46.

[6] 988 F.3d 8 (1st Cir. 2021).

[7] CBP's search policy distinguishes between "advanced" searches of devices, which involve the use of external equipment, such as forensic software, and "basic" searches, which do not. *See* Alasaad v. Nielsen, 419 F. Supp. 3d 142, 148–49 (D. Mass. 2019). "Advanced" and "forensic" are often used interchangeably; the First Circuit in *Alasaad* noted that though the terms may not be "precisely co-extensive," any difference was "immaterial" to the case. *Alasaad*, 988 F.3d at 13 n.3.

[8] *Alasaad*, 988 F.3d at 19–21 (acknowledging that extending the border search exception beyond actual interdiction of contraband to mere evidence of contraband and of border-related crime is contrary to the Ninth Circuit's "narrow view," *id.* at 21 (citing United States v. Cano, 934 F.3d 1002, 1018–19 (9th Cir. 2019))).

missed an opportunity to recognize that "basic" device searches should be considered nonroutine, but also overstated the governmental interests in the border search context, resulting in an interpretation of the Fourth Amendment that threatens individuals' privacy interests at the border.

In July 2017, U.S. citizens Ghassan and Nadia Alasaad were driving home from a vacation in Canada when U.S. Customs and Border Protection (CBP) pulled them aside at a border checkpoint.[9] Officers detained the Alasaad family for six hours.[10] They manually searched Mr. Alasaad's unlocked phone and ordered Ms. Alasaad to provide the password to her locked phone.[11] Ms. Alasaad objected — relenting only after an officer said her phone would be confiscated otherwise.[12] When Mr. Alasaad asked why they were being detained and searched, a supervisor responded that "he had simply felt like ordering a secondary inspection."[13] Later faced with the choice of departing without their phones or waiting several more hours with their daughter, who was ill, the Alasaads chose to leave.[14] Their phones were returned fifteen days later with some media files missing.[15]

Border searches are primarily the responsibility of CBP and U.S. Immigration and Customs Enforcement (ICE).[16] Both CBP and ICE distinguish between "basic" and "advanced" searches of electronic devices: the latter involve the use of external equipment, while the former cover all other searches.[17] Under the agencies' policies, neither type of search requires a warrant: "advanced" searches require reasonable suspicion, and "basic" searches do not require any showing of cause.[18]

The Alasaads and nine other travelers[19] filed suit in the U.S. District Court for the District of Massachusetts, challenging the constitutionality of their searches and CBP's and ICE's search policies on Fourth

---

[9] Amended Complaint ¶¶ 14, 62, 64, *Alasaad*, 419 F. Supp. 3d 142 (No. 17-cv-11730). Judge Casper did not "recount[] the nature and circumstances of all of the Plaintiffs' searches" as she found "a sample of them [to be] illustrative." *Alasaad*, 419 F. Supp. 3d at 149.

[10] Amended Complaint, *supra* note 9, ¶ 71.

[11] *Id.* ¶¶ 65, 67.

[12] *Id.* ¶¶ 67–68. Ms. Alasaad objected because her phone contained images of herself without the headscarf that she wears in public in accordance with her religious beliefs and photos of her daughters that she did not want any CBP officers to view. *Id.* ¶ 67.

[13] *Id.* ¶ 66.

[14] *Id.* ¶¶ 63, 70.

[15] *Id.* ¶ 72. The missing files included videos of their daughter's graduation. *Id.*

[16] Alasaad v. Nielsen, 419 F. Supp. 3d 142, 148 (D. Mass. 2019).

[17] *Id.* at 148–49. CBP and ICE adopted their current policies, including the distinction between "basic" and "advanced" searches, in January 2018 and May 2018, respectively. *Id.* at 164. Though the plaintiffs filed suit in 2017, *id.* at 149, most of their searches can be characterized as "basic," *see id.* at 164.

[18] *See id.* at 148–49.

[19] Of the eleven plaintiffs, ten are U.S. citizens and one is a lawful permanent resident. *Id.* at 147. All had their devices searched at the border without probable cause at least once. *Id.* at 149.

Amendment and First Amendment grounds.[20] Judge Casper denied the government's motion for summary judgment, holding that the agencies' policies violated the Fourth Amendment to the extent that the searches did not require reasonable suspicion of contraband.[21] She acknowledged that the long-standing border search exception recognizes that the government's "interest in preventing the entry of unwanted persons and effects is at its zenith" at the border,[22] based on the "right of the sovereign to control . . . who and what may enter the country."[23] However, Judge Casper reasoned that the border search exception is limited to circumstances where the search "furthers the underlying purpose of the exception,"[24] and that in the context of unwanted effects, the government's "paramount" interests are limited to the actual interdiction of contraband, rather than the "mere evidence of contraband"[25] or "evidence of past or future crimes."[26] Moreover, Judge Casper explained that the border search exception's allowance for suspicionless searches applies only to "routine" searches,[27] while reasonable suspicion is required for "nonroutine" searches.[28] Citing *Riley v. California*,[29] she determined that searches of electronic devices involve intrusions on an individual's privacy that are so significant that they are incomparable to searches of physical items.[30] Given that both "basic" and "advanced"

---

[20] *Id.* at 147. The plaintiffs' First Amendment claim rested on the theory that warrantless searches of electronic devices, which contain personal communications and expressive material, impermissibly burden free speech and association rights. *Id.* at 168–69.

[21] *Id.* at 147–48, 168. Relatedly, she held that any seizure of a device must be for a "reasonable period that allows for an investigatory search for contraband" to comport with the Fourth Amendment. *Id.* at 170. She did not rule on the First Amendment claim specifically, as she determined that the same standard applies under both the First and Fourth Amendments in this context. *See id.*

[22] *Id.* at 156 (quoting United States v. Flores-Montano, 541 U.S. 149, 152 (2004)).

[23] *Id.* at 155 (quoting United States v. Ramsey, 431 U.S. 606, 620 (1977)). A warrantless search is per se unreasonable under the Fourth Amendment, unless a recognized exception applies — including exigent circumstances, searches incident to arrest, vehicle searches, and border searches. *Id.* at 154–55 (citing United States v. Cano, 934 F.3d 1002, 1011 (9th Cir. 2019)).

[24] *Id.* at 157.

[25] *Id.* at 156 (citing *Cano*, 934 F.3d at 1016–18). For instance, searches for contraband, like smuggled firearms, would fall within the exception, but searches seeking to turn up evidence of contraband, like photographs of such weapons, would not.

[26] *Id.* at 166. The distinction between contraband and evidence of related crimes can be subtle. For instance, child pornography discovered on a defendant's laptop can be both contraband itself and evidence of various crimes — including possession of child pornography — but border officials have no authority to search for "evidence that [the defendant] was involved in sex-related crimes generally." *Cano*, 934 F.3d at 1017.

[27] *Alasaad*, 419 F. Supp. 3d at 159 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985)).

[28] *Id.* (quoting United States v. Molina-Gómez, 781 F.3d 13, 19 (1st Cir. 2015)).

[29] 573 U.S. 373 (2014). *Riley* held that warrantless searches of arrestees' cell phones do not fall within the scope of the search-incident-to-arrest exception because they do not further the exception's underlying purposes of mitigating the risk of harm to officers from material concealed on an arrestee's person or the risk of destruction of evidence. *See id.* at 386.

[30] *Alasaad*, 419 F. Supp. 3d at 163 (quoting *Riley*, 573 U.S. at 395–96).

device searches can reveal a wealth of personal information,[31] the district court concluded that any border device search — beyond a cursory look[32] — is a nonroutine search requiring reasonable suspicion of the presence of contraband.[33]

The First Circuit affirmed in part,[34] vacated in part, and reversed in part.[35] Writing for a unanimous panel, Judge Lynch[36] concluded that CBP's and ICE's search policies were constitutional both facially and as applied to the plaintiffs.[37] First, the court held that border searches of electronic devices do not require a warrant or probable cause.[38] Second, the panel held that "basic" searches, as defined by CBP and ICE, do not require reasonable suspicion.[39] Third, the court rejected a contraband-only limit on the scope of the border search exception.[40] The First Circuit traced the exception to the government's "paramount interest in protecting[] its territorial integrity," which overshadows individuals' lowered expectations of privacy at the border.[41]

The First Circuit disagreed with the district court's characterization of the interests implicated by "basic" device searches at the border, instead finding that such searches are routine.[42] Though privacy concerns raised by electronic-device searches may be "significant or novel," the panel noted that they are not as intrusive as the kinds of searches deemed nonroutine, which typically involve searches of a person instead of property.[43] The panel therefore concluded that "basic" device searches do not require reasonable suspicion.[44] Moreover, the panel found that the government's interests at the border extend beyond preventing the entry of contraband to preventing the entry of "*anything*

---

[31] *Id.* at 163, 165. The court explained that the plaintiffs were subject to a broad range of "basic" searches implicating attorney-client communications, journalistic work product, private photos, personal contacts, and other sensitive information. *Id.* at 161, 164.

[32] The court did not dispute that a "cursory search" — namely, "a brief look reserved to determining whether a device is owned by the person carrying it across the border, confirming that it is operational and that it contains data" — would require no showing of cause. *Id.* at 163.

[33] *Id.* at 163–66. Examples of digital contraband provided by CBP and ICE include child pornography, classified information, and counterfeit media. *Id.* at 158.

[34] The First Circuit affirmed the district court's denial of the plaintiffs' motion for summary judgment on the First Amendment claim. *Alasaad*, 988 F.3d at 22–23.

[35] The First Circuit disagreed with the district court, finding the searches and seizures of the plaintiffs' devices, as well as the agencies' policies, to be constitutional. *Id.* at 12.

[36] Judge Lynch was joined by Judge Selya and Judge Laplante of the District of New Hampshire, sitting by designation.

[37] *Alasaad*, 988 F.3d at 12.

[38] *Id.* at 18.

[39] *Id.* at 18–19.

[40] *Id.* at 19–21.

[41] *Id.* at 16 (quoting United States v. Flores-Montano, 541 U.S. 149, 153 (2004)).

[42] *See id.* at 18–19.

[43] *See id.* at 18.

[44] *Id.* at 19.

harmful."[45] Thus, in the court's view, "advanced" border searches of electronic devices may be used not only to interdict contraband, but also to search for "evidence of either contraband or a cross-border crime."[46]

In *Alasaad*, the First Circuit advanced one of the most expansive interpretations of the border search exception amidst a circuit split. Under existing precedent, the court should have categorized all "basic" device searches beyond a cursory look as nonroutine searches requiring reasonable suspicion. The court should have further considered that long-standing precedent limits a nonroutine search to the actual interdiction of contraband, not the mere evidence of contraband or of other crimes. By failing to do so, the First Circuit broadened the scope of government authority to search electronic devices at the expense of individuals' Fourth Amendment interests.

Existing Supreme Court precedent, including *Riley*, leaves open the opportunity to find that all "basic" device searches are nonroutine and therefore require reasonable suspicion. The First Circuit was misguided in restricting nonroutine searches to those that "involve an intrusive search of a *person*."[47] While the Supreme Court's earliest examples of "nonroutine border searches" included "strip, body-cavity, or involuntary x-ray searches,"[48] the Court has recognized two other categories of nonroutine searches that similarly encroach on the dignity and privacy interests of the person subject to search: destructive searches of *property* and searches conducted in a "particularly offensive manner."[49] The Supreme Court has disfavored a balancing test,[50] but lower courts have looked to a variety of factors to determine whether a search is nonroutine, including "the overall manner in which the search is conducted" and "whether the [individual's] reasonable expectations of privacy, if any, are abrogated by the search."[51] *Riley* sheds light on expectations of privacy in the digital context. Though the First Circuit cabined *Riley* to the search-incident-to-arrest exception,[52] both arrestees and travelers at the border share diminished expectations of privacy amid significant, but narrow, governmental interests. *Riley*'s analysis of manual cell phone searches thus should remain instructive even at the border.

A "basic" device search can be just as intrusive as an "advanced" search, so designating the former as routine but the latter as nonroutine is untenable. The First Circuit claimed that there are practical limits to

---

[45] *Id.* at 20 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 544 (1985)).

[46] *Id.* at 19.

[47] *Id.* at 18.

[48] *Montoya de Hernandez*, 473 U.S. at 541 n.4.

[49] United States v. Flores-Montano, 541 U.S. 149, 154 n.2 (2004) (quoting United States v. Ramsey, 431 U.S. 606, 618 n.13 (1977)); *see also id.* at 152–56; Rowland, *supra* note 4, at 548.

[50] *See Flores-Montano*, 541 U.S. at 152.

[51] United States v. Braks, 842 F.2d 509, 512 (1st Cir. 1988) (collecting cases).

[52] *See Alasaad*, 988 F.3d at 17.

the quantity of information accessible during a "basic" search, such as the fact that an officer must "manually traverse the contents of the traveler's electronic device."[53] However, such limits lose all meaning when CBP is able to detain travelers for six hours or retain seized devices for fifteen days. In addition, the information available from device searches is unique in not only its quantity but also its quality.[54] Rejecting an analogy between a search of a cell phone and a search of a "container" with physical contents, the *Riley* Court emphasized that a phone can be "used to access data located elsewhere," revealing information that may not even be turned up by "the most exhaustive" search of a home.[55] Indeed, the thrust of why a device search contravenes an individual's reasonable expectation of privacy lies in the exposure of "a digital realm that is removed both in time and space from the physical locale of the search."[56] Empirically, even purportedly "basic" device searches are seen by ordinary people "as among the most intrusive [searches] contemplated or recorded in the current case law" — "only less embarrassing than strip searches and body cavity searches" but "the *most* revealing of sensitive information."[57] Thus, any device search beyond a cursory look should be considered nonroutine.

The benefits of requiring reasonable suspicion for all device searches beyond a cursory look outweigh efficiency costs. Requiring reasonable suspicion for "basic" searches is not far from the existing practice of border agents, who cannot search every device and therefore already in practice rely on some degree of suspicion in choosing whom to search.[58] Mandating that such suspicion be individualized and reasonable would limit executive discretion and "protect[] citizens against arbitrary, discriminatory, and harassing searches."[59] The Supreme Court has also expressed a "general preference to provide clear guidance to law enforcement through categorical rules."[60] This helped justify the Court's

---

[53] *Id.* at 18.

[54] *See* Alasaad v. Nielsen, 419 F. Supp. 3d 142, 163 (D. Mass. 2019) (citing Riley v. California, 573 U.S. 373, 395–96 (2014)).

[55] *Riley*, 573 U.S. at 396–97.

[56] Tom Rechtin, Note, *Back to the Future of Your Laptop: How Backlash over Prolonged Detention of Digital Devices in Border Searches Is Symptomatic of a Need for "Reasonable Suspicion" in All Border Searches of Digital Devices*, 7 CRIT 66, 89 (2014).

[57] Matthew B. Kugler, Comment, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165, 1196 (2014). The study asked nearly 300 participants to rate the intrusiveness of different border search scenarios; only one of the thirteen scenarios involving electronic devices constituted an "advanced" search. *See id.* at 1192–94.

[58] *See* United States v. Cotterman, 709 F.3d 952, 967 n.14 (9th Cir. 2013); Eunice Park, *The Elephant in the Room: What Is a "Nonroutine" Border Search, Anyway? Digital Device Searches Post-*Riley, 44 HASTINGS CONST. L.Q. 277, 305 (2017).

[59] Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 267 (2011).

[60] *Riley*, 573 U.S. at 398.

bright-line approach in *Riley*, where it steered clear of "assigning law enforcement officers the task of determining which type of cell phone data was searchable incident to arrest, or in what situations specific types of data might be searchable,"[61] observing that this would provide "no practical limit at all."[62] Recognizing that "basic" and "advanced" searches are both nonroutine searches requiring reasonable suspicion would render the border search doctrine more pragmatic.

The First Circuit should have further recognized that the scope of the border search exception for nonroutine searches must be circumscribed by the exception's immigration and customs enforcement purposes. Though the Supreme Court has deemed *routine* searches at the border "reasonable simply by virtue of the fact that they occur at the border,"[63] courts have long assessed the constitutionality of nonroutine border searches by balancing an "individual's Fourth Amendment interests" against the "legitimate governmental interests" at issue.[64] The Supreme Court has traced the government's interests at the border to "the long-standing right of the sovereign to protect itself by stopping and examining *persons* and *property*" in order to "control . . . *who* and *what* may enter the country."[65] Quoting from the Court's most recent border search ruling in *United States v. Flores-Montano*,[66] the *Alasaad* court argued: "[T]he government's interest in preventing crime at international borders 'is at its zenith,' and it follows that a search for evidence of either contraband or a cross-border crime furthers the purposes of the border search exception."[67] The *Flores-Montano* Court, however, had identified the government's interest "at its zenith," to be "preventing the entry of unwanted persons and effects,"[68] not preventing crime generally. With this subtle shift in focus, the First Circuit widened the scope of an intentionally narrow exception. This move is unsupported by precedent and concerning in the Fourth Amendment context, where individual liberty interests are at stake.

Moreover, the First Circuit should have followed the district court in recognizing that *Alasaad* concerned only the government's interest in excluding unlawful property, or contraband. When "U.S. persons" — citizens and lawful permanent residents — are present at the border, as

---

61 Park, *supra* note 58, at 301.

62 *Riley*, 573 U.S. at 399.

63 United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004) (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977)).

64 United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) (quoting United States v. Villamonte-Marquez, 462 U.S. 579, 588 (1983)).

65 *Ramsey*, 431 U.S. at 616, 620 (emphases added).

66 541 U.S. 149 (2004).

67 *Alasaad*, 988 F.3d at 19 (citation omitted) (quoting *Flores-Montano*, 541 U.S. at 152).

68 *Flores-Montano*, 541 U.S. at 152.

in *Alasaad*, the government's right to prevent the unlawful entry of persons loses relevance. Rather, U.S. persons are typically admissible once their identities as citizens or permanent residents have been established.[69] Thus, the scope of the border search exception as applied to U.S. citizens and residents hinges largely on the government's interest in excluding property. In the context of property, the Court has long tethered the government's border search powers to detecting contraband, including by invoking the customs law passed by the First Congress.[70] Lower courts have followed suit in rooting the border search authority over property in customs enforcement, rather than general law enforcement.[71] Extending this limit to the digital realm, the Ninth Circuit in *United States v. Cano*[72] required reasonable suspicion of the presence of digital contraband for nonroutine device searches.[73] By declining to do the same in *Alasaad*, the First Circuit introduced an unprecedentedly broad interpretation of the border search exception.

Involving searches both in the administrative context and at the border, *Alasaad* sits at the intersection of two areas of the law that have received constitutionally exceptional treatment by courts.[74] Given the increasingly fractured nature of the border search doctrine with respect to electronic devices, the Supreme Court may seek to clarify the constitutional limits on such searches — or Congress could "choose to grant greater protection than required by the Constitution."[75] In the meantime, courts seeking to adapt a centuries-old search doctrine to the modern context should recognize the tremendously invasive potential of even "basic" device searches and work to carry forward long-standing limits on the government's search powers at the border.

---

[69] Alasaad v. Nielsen, 419 F. Supp. 3d 142, 158 (D. Mass. 2019). *But see* Donohue, *supra* note 2, at 1013 (noting that admissibility also depends on "arrest alerts or other warrant notifications").

[70] *See* United States v. Molina-Isidoro, 884 F.3d 287, 296 n.7 (5th Cir. 2018) (Costa, J., specially concurring) (collecting cases); *see also Flores-Montano*, 541 U.S. at 153; United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985); *Ramsey*, 431 U.S. at 616–17.

[71] *See, e.g.*, United States v. Kolsuz, 890 F.3d 133, 143 (4th Cir. 2018) (analogizing the case, which concerned the export of contraband, to cases concerning the import of contraband, and distinguishing it from "a case . . . in which the government invokes the border exception on behalf of its generalized interest in law enforcement and combatting crime"); United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013) (noting that "legitimate concerns about child pornography do not justify unfettered crime-fighting searches or an unregulated assault on citizens' private information").

[72] 934 F.3d 1002 (9th Cir. 2019).

[73] *Id.* at 1007, 1014–16.

[74] *See, e.g.*, Philip Mayor, Note, *Borderline Constitutionalism: Reconstructing and Deconstructing Judicial Justifications for Constitutional Distortion in the Border Region*, 46 HARV. C.R.-C.L. L. REV. 647, 647 (2011); Primus, *supra* note 59, at 257.

[75] *Alasaad*, 988 F.3d at 20. Senators Ron Wyden and Rand Paul recently reintroduced the Protecting Data at the Border Act, S. 2957, 117th Cong. (2021), which would require a warrant supported by probable cause to search the electronic devices of U.S. citizens and lawful permanent residents. Press Release, Sen. Ron Wyden, Wyden, Paul Bill Requires Warrants to Search Americans' Digital Devices at the Border (Oct. 7, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-paul-bill-requires-warrants-to-search-americans-digital-devices-at-the-border-2021 [https://perma.cc/SQ2Z-B2S8].