Constitutional Law—Device Searches Absent Reasonable Suspicion Allow Security Interests to Outweigh Privacy Concerns and Amplify Bias at the U.S. Border—Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir. 2021)

Shannah Colbert
_Suffolk University_
CONSTITUTIONAL LAW—DEVICE SEARCHES ABSENT REASONABLE SUSPICION ALLOW SECURITY INTERESTS TO OUTWEIGH PRIVACY CONCERNS AND AMPLIFY BIAS AT THE U.S. BORDER—ALASAAD V. MAYORKAS, 988 F.3D 8 (1ST CIR. 2021)

The Constitution of the United States sets forth fundamental principles that create a national government, divide its power, and protect individual liberties.1 Although the Fourth Amendment forbids unreasonable searches and seizures, some searches, such as those conducted at the United States border, are subject to exceptions.2 In Alasaad v. Mayorkas,3 the United States Court of Appeals for the First Circuit considered whether searches of electronic devices at the border require a warrant.4 Elevating security interests above privacy concerns, the First Circuit held that searches of cellphones and electronic devices fall within the border exception to the

---


2 See U.S. Const. amend. IV (establishing right to privacy against unreasonable searches and seizures). The Fourth Amendment 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, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id.; see also Deborah Anthony, The U.S. Border Patrol’s Constitutional Erosion in the “100-Mile Zone,” 124 Penn St. L. Rev. 391, 396 (2020) (stating different constitutional protections exist for purposes of border security). At the border, “protections against governmental privacy incursions are significantly reduced.” Anthony, supra, at 391 (outlining Supreme Court jurisprudence regarding Fourth Amendment protections and border security); see also Ralph Seep, What constitutes functional equivalent of border for purpose of border exception to requirements of Fourth Amendment, 94 A.L.R. Fed. 372 § 2(a) (2021) (providing background for border search exception).

Historically, border searches have constituted an exception to the Fourth Amendment’s probable cause and warrant requirements. The Supreme Court has noted 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 has entered into the country from outside.

Seep, supra.

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

4 See id. at 12-13 (providing overview of case).
Fourth Amendment’s warrant requirement when such searches are for the purpose of locating contraband or evidence of contraband.5 From 2016 through 2019, at various United States ports of entry, federal officers seized and searched the electronic devices of ten lawful citizens and one permanent resident (“Plaintiffs”).6 While some searches occurred at border crossings, most took place at United States airports as individuals returned from international flights.7 The searches included smartphones, both locked and unlocked, along with other electronic devices such as laptop computers.8 United States Customs and Border Protection (“CBP”) officers searched the devices of five of the Plaintiffs more than once, and CBP officers searched the devices of two female Plaintiffs despite their religious objections to having the officers view photos of the women without their headscarves.9 Information gleaned from the devices notably

5 See id. at 13 (holding basic and advanced searches at border are routine and do not require reasonable suspicion); United States v. Cano, 934 F.3d 1002, 1016 (9th Cir. 2019) (holding manual searches of electronic devices are reasonable without individualized suspicion); United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018) (reiterating routine searches at border do not require reasonable suspicion). The court went on to state that “the district court erroneously narrowed the scope of permissible searches of such equipment at the border.” Alasaad, 988 F.3d at 13; see also HILLEL SMITH & KELSEY SANTAMARIA, CONG. RSCH. SERV., R46601, SEARCHES AND SEIZURES AT THE BORDER AND THE FOURTH AMENDMENT 55 (2021), https://perma.cc/YNM8-XV3E (raising issue of “whether the Supreme Court’s reliance on ethnic appearance as a factor in border-related searches and seizures can still hold sway”). Given changing demographics, several courts have looked to the Fourth Amendment to temper the government’s consideration of ethnicity and race during border stops and detentions. See Smith, supra, at 55-56 (pointing to constitutional challenges). In one case,

[A] federal district court considered a constitutional challenge to the detention of two airline passengers that was based, in part, on their Arab ethnicity. . . . The court declared that ethnicity “has no probative value in a particularized reasonable-suspicion or probable cause-determination” because it has no bearing on a person’s propensity to commit a crime.

Id. at 56; Farag v. United States, 587 F. Supp. 2d 436, 443 (E.D.N.Y. 2008) (rejecting value of race and ethnicity as factor for establishing reasonable suspicion).


7 See Alasaad, 419 F. Supp. at 149 (identifying where searches at issue occurred); see also United States v. Molina-Gómez, 781 F.3d 13, 19 (1st Cir. 2015) (holding border search exception applies to international airports). “International airports . . . are considered the ‘functional equivalent’ of an international border” and are therefore included in the border search exception. See Molina-Gómez, 781 F.3d at 19.

8 See Alasaad, 419 F. Supp. 3d at 149 (describing types of electronic devices searched). At least three plaintiffs had other electronic devices such as a laptop searched. Id.

9 See id. at 149-50 (acknowledging unique circumstances of particular searches). Two of the plaintiffs, Alasaad and Merchant, opposed having male officers view photos of them “without their headscarves as required in public.” Id. at 149.
included highly sensitive work-related materials and privileged attorney-client communications.  

The Plaintiffs filed suit against the heads of the Department of Homeland Security (“DHS”), CBP, and United States Immigration and Customs Enforcement (“ICE”) in their official capacities seeking declarative and injunctive relief, arguing that agency policies concerning electronic devices violated their constitutional rights.  

Plaintiffs first argued that under the Fourth Amendment, the border search warrant exception does not extend to the searches of electronic devices. As to their First Amendment claim, the Plaintiffs alleged that searches of electronic devices without a warrant or reasonable suspicion may chill free speech and interfere with their freedoms related to association and the press. The United States District Court for the District of Massachusetts granted summary judgment in favor of the Plaintiffs’ Fourth Amendment claims, concluding that the CBP and ICE policies violated the Fourth Amendment because basic and advanced searches are non-routine searches that require reasonable suspicion. On appeal, the United States Court of Appeals for the First Circuit held that the border search exception to the warrant requirement “encompassed basic, routine

---

10 See id. at 150 (offering additional examples of searches’ content). One plaintiff’s phone stored information pertaining to his work as a journalist. Id. Another plaintiff’s phone was “a work phone officially owned by NASA” and contained work-related information. Id. A third plaintiff declined to give consent to a search of her phone because it contained attorney-client communications, however, officers proceeded to search her device. Id.  

11 See Alasaad, 988 F.3d at 14-15 (summarizing plaintiffs’ claims). The plaintiffs alleged that the nature of the searches conducted by CBP and ICE violated their Fourth and First Amendment rights. Id. at 14.  

12 See id. at 17 (outlining plaintiffs’ Fourth Amendment claims). The plaintiffs reasoned that the purpose of border search warrant exceptions is limited to “interdicting contraband and preventing the entry of inadmissible persons.” Id. Therefore, expanding the exception to include searches of electronic devices was overly broad and “[does] little to advance the underlying purposes of the border search exception . . . .” Id.  

13 See id. at 21-22 (reasoning warrantless and searches without suspicion threaten sensitive and personal data). The plaintiffs additionally argued that the searches could interfere with their freedom to associate without government scrutiny. Id.  

14 See Alasaad, 419 F. Supp. 3d at 163, 165, 168 (noting breadth of both basic and advanced searches make them non-routine); Alasaad, 988 F.3d at 15 (reviewing procedural posture of case). According to CBP and ICE policies, “a basic search and advanced search differ only in the equipment used to perform the search and certain types of data that may be accessed with that equipment, but otherwise both implicate the same privacy concerns.” Alasaad, 419 F. Supp. 3d at 163 (emphasis added). Basic searches encompass content that is “physically resident” on electronic devices, while advanced searches allow officers to examine deleted and encrypted files as well as employ additional equipment, techniques, and procedures to copy the uncovered information. Id. at 163, 165.
searches of cellphones and electronic devices without reasonable suspicion.”

Fourth Amendment jurisprudence recognizes several exceptions to the warrant requirement. To determine whether a search is exempt from the warrant requirement, courts assess the level of intrusion upon an individual’s privacy and the government’s need to serve a legitimate government interest. Rooted in the government’s “inherent authority to protect,” the border search exception allows for routine searches at the border without a warrant or probable cause. Prior to Congress’ proposal of the Fourth Amendment, Congress implemented the first customs statute, the Act of July 31, 1789, which granted officials the authority to search ships and vessels suspected of concealing goods subject to duty. Because “[a] port of entry is not a traveler’s home[,]” individuals had a lessened expectation of privacy, permitting border searches to enforce duty collection and obtain contraband

---

15 See Alasaad, 988 F.3d at 19-20 (holding electronic device searches at border do not require reasonable suspicion). The court agreed with the holdings of the Ninth and Eleventh Circuits that “basic border searches” of electronic devices are routine and therefore do not impose the requirement of reasonable suspicion. Id.

16 See George C. Thomas III, Stumbling Toward History: The Framers’ Search and Seizure World, 43 TEX. TECH L. REV. 199, 202 (noting Supreme Court’s early recognition of particular exceptions to warrant requirement). Likewise, searches at the border are long recognized as necessary procedures; exemplified by an 1863 act that authorized examination of ships, vessels, and persons to find prohibited goods. Boyd v. United States, 116 U.S. 616, 622-23 (1886); see also Carroll v. United States, 267 U.S. 132, 153-54 (1925) (noting travelers may be stopped at international boundaries to identify themselves and their belongings).


19 See 19 U.S.C.A. § 1595 (originally enacted as Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43) (establishing authority for warrantless searches for illegal goods by custom officials at checkpoints); Ramsey, 431 U.S. at 616 (explaining historical background of border search exception). The Act notably distinguished searches at the border from searches in homes, buildings, or other private dwelling places within the country. Ramsey, 431 U.S. at 616 (differentiating border searches from those under more private circumstances).
without a warrant or probable cause.\textsuperscript{20} As Fourth Amendment jurisprudence evolved, the Supreme Court applied the border search exception’s rationale—that the government’s national security interest outweighs an individual’s expectation of privacy at the border—to modern counterparts, eventually leading lower courts to examine its application to electronic devices.\textsuperscript{21}

The scope of routine and non-routine searches, of which the latter requires reasonable suspicion, is dependent on the degree of invasiveness or intrusiveness of the search and is particular to the facts of a case.\textsuperscript{22} However, the Supreme Court impliedly limited the distinction between routine and non-routine searches to those of persons and not property.\textsuperscript{23} While courts consider the objective intrusiveness of a search, efforts to strike a balance between national security and privacy concerns frequently favor the government’s goal of preventing unwanted individuals and items from entering the country.\textsuperscript{24}

The digital age quickly complicated the reasonableness of border searches, with millions of individuals traveling each day with electronic

\textsuperscript{20} See Ramsey, 431 U.S. at 618 (quoting United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971)) (noting long-standing rationale for border exception); see also Flores-Montano, 541 U.S. at 153-55 (accounting for congressional intent with respect to customs officials).

\textsuperscript{21} See Carroll, 267 U.S. at 154 (explaining nation’s self-protection interest reasonably requires conducting automobile searches at U.S. border); Ramsey, 431 U.S. at 614-15, 624-25 (upholding constitutionality of search of envelopes suspected to contain contraband that arrived from Thailand); see also United States v. Ickes, 393 F.3d 501, 503 (4th Cir. 2005) (finding border search exception gave officials authority to search video camera for contraband); United States v. Saboonchi, 990 F. Supp. 2d 536, 539 (D. Md. 2014) (requiring reasonable suspicion for searches of digital device’s imaged hard drives).

\textsuperscript{22} See United States v. Braks, 842 F.2d 509, 512 (1st Cir. 1988) (listing factors used to determine whether search is routine). Factors to consider include:

(i) whether the search results in the exposure of intimate body parts or requires the suspect to disrobe; (ii) whether physical contact between Customs officials and the suspect occurs during the search; (iii) whether force is used to effect the search; (iv) whether the type of search exposes the suspect to pain or danger; (v) the overall manner in which the search is conducted; and (vi) whether the suspect’s reasonable expectations of privacy, if any, are abrogated by the search.

\textsuperscript{23} See Flores-Montano, 541 U.S. at 152 (suggesting distinction between searches should be reserved to searches of individuals). “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.” Id.

\textsuperscript{24} See id. (stating border exception, while not limitless, recognizes reduced right to privacy at border); see also United States v. Montoya de Hernandez, 473 U.S. 531, 539-40 (1985) (taking account of search’s nature to favor government interests).
devices which contain ranges of sensitive and private information. When examining the constitutionality of a warrantless search of a cellphone incident to a lawful arrest, the Supreme Court acknowledged the unique privacy concerns regarding the search and seizure of information stored in electronic devices. Courts across the circuits have agreed that searches of electronic devices are incomparable to physical items or persons due to the vast amount of accessible information that such devices contain. However, the Supreme Court has declined to “either create or suggest a categorical rule to the effect that the government must always secure a warrant before accessing the contents of such a device.”

Despite continued technological advancements increasing the government’s reach into private data, the Supreme Court has not explicitly addressed the scope of advantaged electronics border searches. Due to the absence of Supreme Court precedent, the United States Courts of Appeals for the Fourth, Ninth, and Eleventh Circuits are split on

---

25 See United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (discussing border search exception’s scope and privacy rights involving electronic devices). “But while technology may have changed the expectation of privacy to some degree, it has not eviscerated it, and certainly not with respect to the gigabytes of data regularly maintained as private and confidential on digital devices.” Id.

26 See Riley v. California, 573 U.S. 373, 393 (2014) (stating modern electronic devices “implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse”). The Court further differentiated electronics “in both a quantitative and a qualitative sense from other objects that might be kept on [a traveler’s] person.” Id. (distinguishing electronic devices); see also Rebecca Rowland, Note, Border Searches of Electronic Devices, 97 WASH. U. L. REV. 545, 559 (2019) (discussing pervasiveness of electronic devices and the frequency with which they accompany travelers to the border); Taylor Hatmaker, Trump Administration Sued Over Warrantless Smartphone Searches at US borders, TECHCRUNCH (Sept. 13, 2017, 3:02 PM), https://perma.cc/JF5K-XUAP (“Our electronic devices contain massive amounts of information that can paint a detailed picture of our personal lives, including emails, texts, contact lists, photos, work documents, and medical or financial records.”)

27 See Cotterman, 709 F.3d at 964 (noting “[e]lectronic devices are capable of storing warehouses full of information”); see also Riley, 573 U.S. at 393 (distinguishing search of cell phones from traditionally searched belongings). “The United States asserts that a search of all data stored on a cell phone is ‘materially indistinguishable’ from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon.” Riley, 573 U.S. at 393.

28 See United States v. Rivera-Morales, 961 F.3d 1, 14 (1st Cir. 2020) (explaining Supreme Court precedent only cautioned application of private search doctrine to electronic devices). The First Circuit determined the Supreme Court’s reasoning in Riley could not be applied to the facts of the case because “a government inspection of evidence that falls within the ambit of the private search doctrine does not constitute a search in the first place[.]” Id.

29 See Cotterman, 709 F.3d at 965 (“With access to the cloud through forensic examination, a traveler’s cache is just a click away from the government.”) The “cloud” allows a user’s data to be held on remote servers as opposed to being on the device itself. Id.; see also United States v. Molina-Isidoro, 884 F.3d 287, 292 (5th Cir. 2018) (noting absence of post-Riley Supreme Court decision requiring warrant for electronic device search).
the level of suspicion required for border searches of electronic devices.\textsuperscript{30} Specifically, the circuits differ on whether the warrant requirement for cellphone searches applies to forensic searches of electronic devices at the border.\textsuperscript{31} The Fourth and Ninth Circuits agree that officers must possess some level of individualized suspicion of criminal activity to perform a search absent a warrant or probable cause.\textsuperscript{32} In contrast, the Eleventh Circuit held that border searches of electronic devices may be performed by officers without reasonable suspicion.\textsuperscript{33}

At the border, CBP and ICE enforce a broad spectrum of laws, and both agencies’ policies provide nearly-identical “standard procedures” for searches of electronic devices to ensure compliance with customs, immigration, and other regulations.\textsuperscript{34} CBP policy specifically demands that officers do not take race or ethnicity into account with border investigation, screening, and law enforcement.\textsuperscript{35} However, a number of suits filed against border

\begin{footnotes}
\item[30] See United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018) (outlining precedent holding forensic searches of electronic devices require individualized level of suspicion); see also Cotterman, 709 F.3d at 957 (concluding reasonable suspicion for forensic searches of electronic devices at border required under circumstances). \textit{But see} United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018) (holding no suspicion required to search electronic devices at border).


\item[32] See United States v. Aigbekaen, 943 F.3d 713, 719 n.4 (4th Cir. 2019) (allowing officers to conduct searches of cellphones at border with reasonable suspicion); \textit{see also Kolsuz,} 890 F.3d at 146-47 (concluding search of electronic device constituted non-routine border search requiring reasonable suspicion); United States v. Cano, 934 F.3d 1002, 1016 (9th Cir. 2019) (holding “manual searches of cell phones at the border are reasonable without individualized suspicion”).

\item[33] See United States v. Vergara, 884 F.3d 1309, 1312-13 (11th Cir. 2018) (holding \textit{Riley} did not change rule to requiring only reasonable suspicion); \textit{Touset,} 890 F.3d at 1233 (“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”). The First Circuit, however, declined to differentiate between a laptop and cellphone, finding reasonable suspicion existed regardless of whether the search was routine. United States v. Molina-Gómez, 781 F.3d 13, 19-20 (1st Cir. 2015). “We need not categorize the search as either routine or non-routine because we agree with the government that even assuming the search was non-routine, reasonable suspicion existed to justify the search.” \textit{Id.}

\item[34] See 6 U.S.C. § 211(c)(5) (listing duty to “detect...respond to...and interdict...persons who may undermine the security of the United States”); \textit{see also CBP Directive No. 3340-049A, Border Search of Electronic Devices} (Jan. 4, 2018), https://perma.cc/495W-EBWN (outlining appropriate procedure for device searches at border); Immigration and Customs Enforcement Directive No. 7-6.1, \textit{Border Searches of Electronic Devices} (Jan. 4, 2018), https://perma.cc/763C-E4AH (providing legal guidance and establishing policy for border search authority). Regardless of whether a search is basic or advanced, officers are authorized to search “information that is resident upon the [electronic] device.” CBP Directive No. 3340-049A, \textit{supra}.

\item[35] See CBP Policy on Nondiscrimination in Law Enforcement Activities and all other Administered Programs, U.S. CUSTOMS AND BORDER PROT. (Feb. 24, 2020), https://perma.cc/F76R-UDJQ (prohibiting consideration of race or ethnicity for almost all CBP activities). CBP further
patrol agencies alleged discriminatory enforcement against people of color. Documented racial profiling confirms that certain racial and religious groups face an increased likelihood of being searched at border stops. For example, CBP arrest records from bus terminals and railway stations in Rochester, New York, reveal that out of 2,776 arrests over four years, only 0.9%

insists the agency “is fully committed to the fair, impartial and respectful treatment of all members of the trade and traveling public.” Id. The DHS similarly implemented a policy that prohibits the use of race or ethnicity under all but extraordinary circumstances. Smith & Santamaria, supra note 5, at 56-57.

According to the agency, immigration officers may consider race or ethnicity only when there is a “compelling governmental interest” present, and the officers exercise their authority “in a way narrowly tailored to meet that compelling interest.” The agency’s policy does not preclude consideration of race or ethnicity if that information is “specific to particular suspects or incidents” (e.g., to identify a suspect).

Id. at 57. But see Hugh Handeyside et al., We Got U.S. Border Officials to Testify Under Oath. Here’s What We Found Out, ACLU (Apr. 30, 2019), https://perma.cc/6CWB-K8WA (suggesting border officials’ behavior does not align with alleged commitment to fairness, equality, and impartiality).

36 See Chris Rickerd, A Dangerous Precedent: Why Allow Racial Profiling at or Near the Border?, ACLU (Dec. 8, 2014), https://perma.cc/ZW7Z-MRHV (asserting CBP’s “horrible track record of discriminatory enforcement against people of color”); Ahad Khilji, Comment, Warrantless Searches of Electronic Devices at U.S. Borders: Securing The Nation or Violating Digital Liberty?, 27 CATH. U. J. L. & TECH. 173, 201 (2019) (contending people of color targeted by CBP agents); see also Memorandum in Support of Defendant at 1, Owunna v. United States, 2018 WL 3342773 (E.D. Va. May 3, 2018) (No. 1:18-cv-00536-LMB-MSN) (noting plaintiff’s claim of improper detainment and device search by CBP); Millan-Hernandez v. Barr, 965 F.3d 140, 149 (2d Cir. 2020) (exemplifying case where evidence suggested racial considerations led to border search). Millan-Hernandez exposed a CBP supervisor’s racial slurs towards Latinos, and an anonymous ICE official stated that there is a “very specific clientele that [they] look for.” 965 F.3d at 149. After stopping the vehicle Millan-Hernandez was a passenger in for a potential traffic violation and learning that the driver had a foreign passport, an officer demanded that all passengers provide their papers. Id. at 148.

37 See Anthony, supra note 2, at 403 (pointing to reports suggesting only non-white passengers subjected to border searches). Evidence also suggests that at one CBP checkpoint, “Latinos were twenty times more likely to be detained than non-Latinos.” Id. at 402. Another report conducted by the ACLU revealed that 85% of individuals apprehended in Michigan between 2012 and 2018 were from Latin America. Joe Davidson, Black Officers Say CBP Forced Them to Profile. A Study in One State Backs Them Up., WASH. POST (July 22, 2021, 6:00 AM), https://perma.cc/9BYP-H6LT (noting being person of color key reason for border control stop); see also Anna Kaplan, Border Agents Caught Engaging With Violent Facebook Posts Given Lighter Punishment Than Recommended, House Report Says, FORBES (Oct. 25, 2021, 2:00 PM), https://perma.cc/PG7Y-6E7B (reporting on border officials’ participation in discriminatory social media activity investigation). The report’s findings revealed CBP agents engaged in “misconduct including degrading and threatening comments about migrants,” as members of private Facebook groups. Kaplan, supra note 37. Beyond traditional checkpoints, CBP and ICE officers have searched and detained these groups at bus terminals, railway stations, and traffic stops within the United States’ borders. Anthony, supra note 2, at 400-02. “In addition to its regular operations at the border and ports of entry, CBP operates approximately 32 permanent ‘interior border checkpoints’ throughout the country, along with another 39 temporary internal or ‘tactical’ checkpoints.” Id. at 400.
involved individuals with a “fair complexion.” Thus, people of color with privacy concerns that are already weakened by security interests are also disproportionately subjected to searches of their electronic devices.

In Alasaad v. Mayorkas, the First Circuit addressed whether the border exception allows agents to perform basic searches of electronic devices without reasonable suspicion. After affirming that border searches do not require a warrant, the court focused on the “novel and significant” privacy concerns surrounding electronic devices. Despite such considerations, the court determined that government interests, which are paramount at the border, outweigh individual privacy concerns.

Further, because there is no “intrusive search of a person” when examining an electronic device, the court held basic border searches of electronic devices are routine and do not require reasonable suspicion. The court credited the border agencies’ guidance, which only permits a manual search of a traveler’s electronic device and prohibits any investigation beyond “data resident on the device,” stating that such policies restrict the scope of private information accessible by an agent and counter concerns regarding deleted or encrypted files that may be especially sensitive. In accordance with previous Ninth and Eleventh

38 See Anthony, supra note 2, at 402-03 (providing statistical evidence of racial profiling at border checkpoints).


40 See Alasaad v. Mayorkas, 988 F.3d 8, 18-19 (1st Cir. 2021) (allowing routine searches of electronic devices at border absent reasonable suspicion of contraband).

41 See id. at 18 (discussing privacy concerns surrounding modern implications of electronic devices). To defend their argument that border searches of electronic devices are non-routine, the plaintiffs contended that electronic devices “may contain a trove of sensitive personal information. Id.; see also Riley v. California, 573 U.S. 373, 393 (2014) (emphasizing privacy concerns’ unique nature); Kyllo v. United States, 533 U.S. 27, 33-34 (2001) (acknowledging impact of technological advancement).

42 See Alasaad, 988 F.3d at 18 (recognizing superiority of government interests); see also Riley, 573 U.S. at 393 (distinguishing electronic devices searches information quantity and quality). While both Alasaad and Riley involved the search of electronic devices, the court noted that “[t]he search incident to arrest warrant exception is premised on protecting officers and preventing evidence destruction, rather than on addressing border crime.” Alasaad, 988 F.3d at 17 (differentiating circumstances of two cases); Riley, 573 U.S. at 384-86 (outlining exception’s priorities).

43 See Alasaad, 988 F.3d at 18 (determining border searches of electronic devices considered routine); see also United States v. Montoya de Hernandez, 473 U.S. 531, 541 n.4 (1985) (providing non-routine search example). Some non-routine searches include strip, body-cavity, and involuntary x-ray searches. Montoya de Hernandez, 473 U.S. at n.4.

44 See Alasaad, 988 F.3d at 18-19 (detailing scope of routine electronic device search and limitations imposed by CBP policy); see also CBP Directive No. 3340-049A, supra note 34 (establishing guidelines for basic border searches of electronic devices).
Circuit rulings, the court concluded that basic border searches of electronic devices may be conducted without reasonable suspicion. 45

The First Circuit also rejected arguments that the border search exception: (1) only extends to searches aimed at preventing the entry of contraband and inadmissible persons; and (2) only includes searches for illegal contraband itself. 46 The court explained that compared to non-border contexts, the scope of warrantless searches at the border “must be limited . . . to that which is justified by the particular purposes served by the exception.” 47

Because the government’s primary intention is to prevent crime at international borders, the court reasoned that searches for evidence of contraband or crime align with that fundamental objective. 48 With respect to the scope of advanced searches, the court suggested that constitutional limitations do not prevent Congress’s authorization of the inclusion of information or items other than contraband. 49 Additionally, the court dismissed the alleged distinction between evidence of contraband and contraband itself, concluding that searches for evidence are critical to the government’s interest in controlling “who and what may enter the country.” 50

While government interests at the border are undoubtedly important, the Alasaad court failed to adequately address Fourth Amendment privacy concerns related to the contents of electronic devices. 51 In particular, the court did not consider the impact of technological advancements discussed

45 See Alasaad, 988 F.3d at 18 (holding border search exception permits basic electronic device searches without reasonable suspicion). “Every circuit that has faced this question has agreed that Riley does not mandate a warrant requirement for border searches of electronic devices, whether basic or advanced.” Id. at 17 (highlighting other circuit court decisions); see also United States v. Vergara 884 F.3d 1309, 1312-13 (11th Cir. 2018) (holding border searches exempt from warrant or probable cause requirement); United States v. Cano, 934 F.3d 1002, 1015-16 (9th Cir. 2019) (holding basic and advanced border searches may be performed without warrant or probable cause).

46 See Alasaad, 988 F.3d at 19 (addressing scope of border search exception). In Alasaad, the plaintiffs argued that the exception does not apply to searches for evidence of border-related crimes or contraband. Id.


48 See id. (proposing evidence of contraband or crime furthers government’s primary purpose). The court also noted that the Supreme Court “has repeatedly said that routine searches ’are reasonable simply by virtue of the fact that they occur at the border.’” Id. (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977)).

49 See id. at 19-20 (doubting any congressional limitation on scope of border search exception). The court goes on to state that “Congress is better situated than the judiciary to identify the harms that threaten us at the border.” Id. at 20.

50 See id. at 20 (denying plaintiffs’ argument given fulfillment of government purpose); see also Ramsey, 431 U.S. at 620 (recognizing exception justified to allow government to control what enters country); United States v. Aigbekaen, 943 F.3d 713, 721 (4th Cir. 2019) (including prevention of contraband introduction as basis for exception).

51 See Alasaad, 988 F.3d at 20 (characterizing electronic device search as unintrusive).
by other circuits. The Fourth Amendment guarantees people the right to be secure in their “papers,” which arguably includes the breadth of information stored on electronic devices. Electronic devices’ capacity to store deleted or encrypted files and the development of cloud computing technology demonstrate the unique and expansive nature of digitally accessible data that warrants certain constitutional protections. Further, the contents stored on electronic devices are starkly different from the contents “traditionally circumscribed by the size of [a] traveler’s luggage or automobile,” for which the border exception was originally conceived. Consequently, “technology matters,” and the scope of discoverable information on electronic devices warrants a heightened expectation of privacy because the search is considerably more intrusive than that of traditional property in a non-routine investigation.

While the court emphasized the government’s heightened security interests, it was reluctant to thoroughly discuss the reasonableness of searches conducted at the border and suggested that Congress and the Executive Branch are better equipped to evaluate potential harms. A careful

52 See United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013) (recognizing nature of electronic devices renders an attendant privacy expectation). This stance “stands in stark contrast to the generic and impersonal” items. Id.
53 See id. (“[electronic devices] contain the most intimate details of our [travelers] lives: financial records, confidential business documents, medical records and private emails.”) The court further stated that the nature of these materials implicates the constitutional protections of the Fourth Amendment providing people the right to be secure in their “papers.” Id.; see also U.S. CONST. amend. IV (guaranteeing right of people to be secure in their papers).
54 See Cotterman, 709 F.3d at 965 (explaining extent of technological advancement).
55 See id. at 964 (recognizing evolving technologies have broadened government intrusion capabilities); Rowland, supra note 26, at 545 (“The border search exception originally was designed to allow border agents to search travelers’ luggage for contraband and other harmful materials. However, with the progress of technology, the border search exception is now being exploited by border agents to conduct forensic searches of travelers’ electronic devices.”) Advancements in technology are also demonstrated by the fact that the number of searches of electronic devices is increasing each year, with over 33,000 searches in 2018. Rowland, supra note 26, at 545.
56 See Cotterman, 709 F.3d at 966 (“Technology has the dual and conflicting capability to decrease privacy and augment the expectation of privacy”; see also Kyllo v. United States, 533 U.S. 27, 33-34 (2001) (“It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”)
57 See Alasaad v. Mayorkas, 988 F.3d 8, 19-20 (2021) (dismissing question of whether searches for items other than contraband are reasonable); see also United States v. Kolsuz, 890 F.3d
examination of competing policy considerations reveals that the Fourth Amendment, at its core, is a reflection of the founders’ concern with government intrusion on private thoughts and ideas, and such concerns should not be ignored simply because one crosses a border.\textsuperscript{58} The modern-day traveler cannot feasibly delete files or leave their electronic device at home to mitigate the government’s intrusion into their private affairs.\textsuperscript{59} Accordingly, implementing the requirement of reasonable suspicion of contraband, or evidence of contraband related to a traveler’s electronic device, could effectively balance the government’s security interests with the individual’s constitutional right to freedom from unreasonable searches and seizures.\textsuperscript{60}

A comprehensive exploration of reasonableness and the scope of searches in this context should also examine the persistent issue of racial bias at the border.\textsuperscript{61} Absent the requirement of a warrant or reasonable suspicion for searches of electronic devices at the border, the harm to groups whose Fourth Amendment rights are already weakened because they are disproportionately subjected to searches at the border will be amplified.\textsuperscript{62} Despite internal nondiscrimination guidance from the Department of Homeland Security (“DHS”), CBP, and ICE, courts continue to waver on whether race and ethnicity can be considered a factor under the guise of “exceptional instances.”\textsuperscript{63}

133, 152 (4th Cir. 2018) (indicating continued uncertainty as to who should strike balance at border).

\textsuperscript{58} See Cotterman, 709 F.3d at 964-65 (emphasizing importance of historical intent of Fourth Amendment). \textit{But see} Alasaad, 988 F.3d at 20 (asserting Congress and Executive branch can implement greater protection of electronic devices at border).

\textsuperscript{59} See Rowland, \textit{supra} note 26, at 558 (“the only certain way to protect against forensic searches of electronic devices at the border is to leave their devices at home entirely – a solution which is impractical in the modern age.”) However, individuals increasingly rely on their electronic devices and leaving them at home is impractical. \textit{Id.; see also} Cotterman, 709 F.3d at 965 (“[R]emoving files unnecessary to an impending trip is an impractical solution given the volume and often intermingled nature of the files.”) The court noted “it is also a time-consuming task that may not even effectively erase the files.” \textit{Cotterman,} 709 F.3d at 965.

\textsuperscript{60} See United States v. Flores-Montano, 541 U.S. 149, 152 (2004) (requiring “some level of suspicion in the case of highly intrusive searches of the person”); \textit{see also} Rowland, \textit{supra} note 26, at 572 (arguing lack of adequate protections makes reasonable suspicion standard imperative to privacy interests). Manual searches and forensic searches implicate a similar level of sensitive information, indicating that manual searches should involve a higher standard of reasonableness. Rowland, \textit{supra} note 26, at 570 (characterizing both searches as nonroutine).

\textsuperscript{61} See Rickerd, \textit{supra} note 36 (citing evidence of racial profiling at various border stops).

\textsuperscript{62} See Flores-Montano, 541 U.S. at 152 (highlighting importance of government’s security interests); Florida v. Bostwick, 501 U.S. 429, 434-35 (1991) (suggesting individuals can counter privacy concerns); \textit{see also} Khilji, \textit{supra} note 36, at 203 (describing increased number of Muslim travelers’ devices being searched); Anthony, \textit{supra} note 2, at 403 (discussing reports of disproportionate searches of certain groups).

\textsuperscript{63} See sources cited \textit{supra}, note 35 (discussing agency commitment to impartial treatment of all persons crossing border); \textit{see also} Smith & Santamaria, \textit{supra} note 5, at 55-57 (examining
Device Searches Amplify Bias at the U.S. Border

2022] Device Searches Amplify Bias at the U.S. Border 307

groups undermine these agencies’ efforts, and recent cases indicate the implementation of agency nondiscrimination standards alone are insufficient to prevent officials from relying on race or ethnicity during border enforcement activities. By reaffirming the dominance of government security interests, the court enables and enhances the likelihood that persons belonging to particular racial and ethnic groups will be subject to searches without reasonable suspicion. In Alasaad, the First Circuit interpreted the border search exception to encompass routine searches of electronic devices without reasonable suspicion of contraband or evidence of contraband. The court’s reluctance to yield to contemporary privacy concerns surrounding electronic devices allowed the court to ignore the need for a standard requiring reasonable suspicion. Rather than uphold the already weakened constitutional rights of marginalized individuals, the First Circuit advanced the potential for increased Fourth and Fourteenth Amendment violations at the United States border.

Shannah Colbert

64 See Hatmaker, supra note 26 (detailing suit against border agents “emboldened” by Trump administration’s travel and immigration policies); see also sources cited supra, note 36 (noting instances where border agents failed to uphold agencies’ nondiscriminatory policies).

65 See Rickerd, supra note 36 (indicating racial profiling will continue to occur at border); Davidson, supra note 37 (“[d]espite the policy, the border Patrol nationally suffers ‘a persistent culture of racism’”); see also Handeyside et al., supra note 35 (“CBP and ICE are asserting near-unfettered authority to search and seize travelers’ devices at the border, for purposes far afield from the enforcement of immigration and customs laws.”)