PRIVACY IN THE DIGITAL AGE:
A CASE FOR A STRICTER, UNIFORM STANDARD FOR SEARCHING
ELECTRONIC DEVICES IN BORDER ZONES

Alex Crowley*

I. Introduction
International travelers to the United States, including lawyers charged with maintaining the confidentiality of client information, need to think twice about traveling with portable electronic devices that contain sensitive information.¹ Travelers entering the United States may believe that border officials need a valid reason to search their electronic devices,² but unfortunately for them, this belief is

* J.D. Candidate, Suffolk University Law School, 2024.
¹ See Daniel Telvock, Investigation: Why are border searches allowed without a warrant?, ROCHESTERFIRST.COM (Oct. 4, 2022), archived at https://perma.cc/F4FC-ZFDX (discussing recent rise in searches of electronics by border officials); FOX 5 Digital DC Team, Can the government search your phone at the airport?, FOX 5 WASH. DC (Sept. 21, 2022), archived at https://perma.cc/VGX5-R68Q (highlighting that border officials do not need a warrant or even probable cause to search one’s electronics); As border searches of electronics rise, here’s how to protect your clients’ data, A.B.A. (Sept. 2017) [hereinafter Protecting Client Data], archived at https://perma.cc/7G7J-A3DL (expressing concern over rise in searches of lawyers’ electronic devices and discussing how to protect against confidentiality breaches).
² See Alasaad v. Mayorkas, 988 F.3d 8, 13–14 (1st Cir. 2021) (summarizing plaintiff’s challenges to policies by U.S. Customs and Border Protection “authorizing warrantless basic searches of electronic devices at border without reasonable suspicion, warrantless advanced searches based on reasonable suspicion, and warrantless detention of devices.”); FOX 5 Digital DC Team, supra note 1 (summarizing Abdulkadir Dur’s challenge to government’s warrantless search and seizure of his electronic devices at the airport).

Copyright © 2024 Journal of High Technology Law and Alex Crowley.
All Rights Reserved. ISSN 1536-7983.
incorrect. One’s level of protection against unreasonable searches of electronic devices by border officials depends entirely on which part of the country they seek to enter.

In *Alasaad* v. *Mayorkas*, the First Circuit held that basic searches of electronic devices in border zones, without a warrant or even reasonable suspicion of criminal activity, do not violate the Fourth Amendment protection against unreasonable searches and seizures. Furthermore, the court held that, while officers must have reasonable suspicion to conduct advanced searches of electronics, border searches of electronic devices do not have to be limited in scope to searches for contraband.

---

3 See *Alasaad*, 988 F.3d at 19–20 (holding that basic border searches do not require reasonable suspicion, and that advanced border searches supported by reasonable suspicion are not limited to searches for contraband); United States v. *Kolsuz*, 890 F.3d 133, 137 (4th Cir. 2018) (holding that basic border searches do not require reasonable suspicion); United States v. *Arnold*, 533 F.3d 1003, 1008 (9th Cir. 2008) (holding that reasonable suspicion not required for customs agents to search a laptop).

4 Compare *Alasaad*, 988 F.3d at 19–20 (deciding that border searches in the First Circuit are not limited in scope to searches for contraband), and *Kolsuz*, 890 F.3d at 142 (holding that border searches in the Fourth Circuit are not limited in scope to searches for contraband), with United States v. *Cano*, 934 F.3d 1002, 1018 (9th Cir. 2019) (holding that border searches in the Ninth circuit must be limited in scope to searches for contraband).

5 See *Alasaad*, 988 F.3d at 19 (holding that basic border searches do not require reasonable suspicion). “We thus agree . . . that basic border searches are routine searches and need not be supported by reasonable suspicion.” *Id.* See also Deborah Anthony, *The U.S. Border Patrol’s Constitutional Erosion in the “100-Mile Zone”*, 124 PENN. ST. L. REV. 391, 398 (2020) (emphasizing that a border zone extends “100 air miles from any external boundary, including all coasts and waterways.”). See also, e.g., *Cano*, 934 F.3d at 1016; United States v. *Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018) (holding that basic border searches are routine searches and need not be supported by reasonable suspicion). See generally U.S. CUSTOMS AND BORDER PROTECTION, BORDER SEARCH OF ELEC. DEVICES, CBP Directive No. 3340-049A, 2–5 (2018) [hereinafter *CBP Policies*] (defining electronic devices and distinguishing between basic searches and advanced searches). “[A]ny device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices . . .” *Id.* at 2. “An advanced search is any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents.” *Id.* at 5. “Any border search of an electronic device that is not an advanced search . . . may be referred to as a basic search.” *Id.* at 4.

6 See *Alasaad*, 988 F.3d at 19–20 (holding that border searches of electronic devices are not limited in scope to searches for contraband); *But see Cano*, 934 F.3d at 1018 (holding that border search exception is restricted in scope to searches for
United States v. Kolsuz, holding that a forensic search of a smartphone is a nonroutine, advanced search and that these searches require reasonable suspicion of criminal activity. Conversely, in United States v. Touset, the Eleventh Circuit held that customs agents do not need any level of suspicion to conduct a search of one’s electronic devices in border zones. Furthermore, in United States v. Cano, the Ninth Circuit held that warrantless searches of electronics must be limited in scope to searches for digital contraband. The lack of agreement among circuits, and lack of clear direction from the Supreme Court, exposes civilians to intrusion depending on which part of the country they seek to enter.

Professionals, especially lawyers, who carry confidential client information on electronic devices are especially at risk. Basic searches of a lawyer’s personal electronic devices can expose sensitive information, including a client’s personal information, litigation contraband). We cannot agree with its narrow view of the border search exception because Cano fails to appreciate the full range of justifications for the border search exception beyond the prevention of contraband itself entering the country.” Alasaad, 988 F.3d at 21.

7 See Kolsuz, 890 F.3d at 144-46 (holding that smartphone searches are nonroutine, and therefore, customs agents need reasonable suspicion to conduct a smartphone search).

8 See Touset, 890 F.3d at 1233 (holding that basic border searches do not require reasonable suspicion).

9 See Cano, 934 F.3d at 1018 (issuing the holding in the case). See also Laura K. Donohue, Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches, 128 YALE L.J. 961, 1009 (2019) (explaining that digital contraband involves “illicit materials that happen to be digitized”). “Child pornography, nuclear weapon designs, and counterfeit currencies, for instance, are all expressly forbidden under customs laws.” Id.

10 Compare Alasaad, 988 F.3d at 19 (deciding that border searches in First Circuit do not have to be limited in scope to searches for contraband), and Kolsuz, 890 F.3d at 142 (holding that border searches in Fourth Circuit territory are not limited in scope to searches for contraband), with Cano, 934 F.3d at 1018 (holding that border searches in Ninth circuit territory must be limited in scope to searches for contraband).

11 See Protecting Client Data, supra note 1 (advising lawyers on how to protect against confidentiality breaches during border searches); Joseph J. Lazzarotti & Maya Atrakchi, ABA Gets Lawyers Heightened Protections for Device Searches at International Borders, JACkSON LEWIS (Jan. 31, 2018), archived at https://perma.cc/2MED-G2CL (emphasizing that border searches of electronic devices pose confidentiality concerns for lawyers); Amanda Robert, Privacy rights of lawyers and their clients should be protected during border searches, ABA House urges, A.B.A. J. (Jan. 28, 2019), archived at https://perma.cc/W8J5-UJD4 (addressing concerns over breaches of attorney-client privilege during border searches).
strategy, and other confidential case information.\textsuperscript{12} A more advanced search of the lawyer’s electronic devices could reveal thousands of pages of privileged documents related to pending cases.\textsuperscript{13} Exposing this information to border officials is a violation of attorney-client privilege, and threatens the integrity of a client’s relationship with their attorney.\textsuperscript{14} In this context, an attorney has a professional obligation to protect against these breaches by guarding against the possibility of these devices being searched.\textsuperscript{15} But how can an attorney reasonably do so when these devices are so pervasive in the legal profession, so important for legal work, store such immense amounts of sensitive information, and are subject to different search standards based on which border zone the lawyer is in?\textsuperscript{16}

Courts established the border search exception, which allows border officials to search travelers and items crossing into the United States without a warrant, during a time when portable electronics did not exist. In the modern world, electronics pervade nearly every aspect of daily life. Furthermore, these devices possess immense storage capacity and hold private, intimate details of one’s personal and professional lives. For this reason, the court’s holding in \textit{Alasaad} contradicts the Fourth Amendment’s protection against unreasonable searches and seizures. All electronics searches in border zones should require a warrant, or in the alternative, reasonable suspicion of criminal activity, because even basic searches can uncover personal, intimate, and sensitive information. Furthermore, electronics searches

\begin{footnotesize}
\begin{enumerate}
\item See Robert, supra note 11 (discussing the potential for breaches of attorney-client privilege during searches of an attorney’s electronic devices).
\item See \textit{CBP Policies}, supra note 5, at 5 (describing the nature of advanced electronic device searches). “An advanced search is any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents.” \textit{Id.} This external equipment used to review, copy, and analyze data grants access to significantly more information, in a shorter period, than does a basic search. \textit{Id.} See also \textit{Protecting Client Data}, supra note 1 (discussing concerns regarding searches of attorneys’ laptops containing privileged information, and the steps taken by the ABA to advocate for more stringent search requirements).
\item See Robert, supra note 11 (emphasizing how protected client information easily becomes available during searches of attorney’s laptops). See also Lazzarotti \& Atrakchi, supra note 11 (discussing violations of attorney-client privilege at international borders).
\item See \textit{Protecting Client Data}, supra note 1 (stating that lawyers must “make reasonable efforts to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation of a client . . . ”).
\item See generally \textit{Protecting Client Data}, supra note 1 (emphasizing that lawyers’ electronic devices likely carry significant amounts of sensitive information).
\end{enumerate}
\end{footnotesize}
should be limited in scope to searches for digital contraband. Otherwise, these searches risk violating one’s constitutional rights.

II. History

A. Origins of Fourth Amendment Jurisprudence

Prior to the American Revolution, British officials commonly issued warrants, also known as writs of assistance, allowing for generalized searches of colonists’ private property. These writs required neither a warrant nor probable cause, and remained active until the death of the British monarch who ruled at the time the writ was issued. The Framers vehemently opposed the issuance of such warrants, and made this opposition abundantly clear. The Framers of the Constitution drafted the Fourth Amendment to protect against


18 See Thomas III, supra note 17, at 206 (detailing characteristics of British writs of assistance). “These searches required neither a warrant nor probable cause. The writs expired only when the monarch expired . . . .” Id.

19 See Meet the Framers of the Constitution, NAT’L ARCHIVES (Mar. 16, 2020), archived at https://perma.cc/2L8H-WFKB (defining the Framers as the appointed delegates who attended the constitutional convention and signed the Constitution). See also Thomas III, supra note 17, at 207 (emphasizing specific instances of Framers’ hostility towards improper searches of private property by government officials). [Patrick] Henry said that . . . “[t]he federal sheriff may commit what oppression, make what distresses, he pleases, and ruin you with impunity; for how are you to tie his hands?” Id. “In a different speech, Henry predicted that ‘any man may be seized, any property may be taken, in the most arbitrary manner, without any evidence or reason.’” Id.

In yet another speech, Henry thundered: The officers of Congress may come upon you now, fortified with all the terrors of paramount federal authority . . . . They may . . . go into cellars and rooms, and search, ransack, and measure, every thing you eat, drink, and wear.

Id.
general searches and seizures of private property by government officials.\(^{20}\)

**B. Scope of the Fourth Amendment**

The Fourth Amendment states,  

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.\(^{21}\)

Under the Fourth Amendment, every search and seizure by a government official must be reasonable.\(^{22}\) The Amendment protects people from unreasonable invasions of their legitimate expectations of privacy.\(^{23}\) The reasonableness of a search depends on the totality of the circumstances, including the nature and purpose of the search and the extent to which it intrudes upon legitimate expectations of

---

\(^{20}\) See Thomas III, *supra* note 17, at 208 (stating that colonists established the Fourth Amendment as a response to oppressive British search tactics). "Writs of assistance were condemned as a ‘detestable instrument of arbitrary power’ that ‘invited capricious house searches by insolent officers of the new central government.’ These were the government actions that the Framers had in mind when they drafted the Fourth Amendment and sent it to the states." *Id.* See also *Stanford*, 379 U.S. at 482 (establishing that Framers established the Fourth Amendment as a response to British search practices). “[T]he Fourth Amendment was most immediately the product of contemporary revulsion against a regime of writs of assistance . . . .” *Id.*

\(^{21}\) See U.S. CONST. amend. IV (laying out the Constitution’s protections against unreasonable searches and seizures).


\(^{23}\) See Elizabeth M. Bosek et al., *§ 127. Federal Constitutional Foundations Respecting Search and Seizure*, 25 Ohio Juris. (2022) (explaining that Fourth Amendment “protects people from unreasonable government intrusions into their legitimate expectations of privacy.”); *Gant*, 556 U.S. at 338 (emphasizing that searches by government officials must be reasonable); *Katz*, 387 U.S. at 351–52 (discussing that the Constitution may protect what one seeks to preserve as private); *Johnson*, 333 U.S. at 14–15 (acknowledging that searches by government officials must be reasonable).
privacy. Generally, a search of private property requires a warrant based on probable cause, or else the search is per se unreasonable. The Supreme Court of the United States has defined several exceptions


25 See Camara v. Mun. Ct. of City and Cnty. of S.F., 387 U.S. 523, 528–29 (1967) (discussing that warrantless searches are unreasonable). “[E]xcept in certain carefully defined classes of cases, a search of private property without proper consent is ‘unreasonable’ unless it has been authorized by a valid search warrant.” Id. See also 18 U.S.C.A. § 2236 (stating that government officials that conduct warrantless searches of private dwellings shall be subject to discipline).

Whoever, being an officer, agent, or employee of the United States or any department or agency thereof, engaged in the enforcement of any law of the United States, searches any private dwelling used and occupied as such dwelling without a warrant directing such search, or maliciously and without reasonable cause searches any other building or property without a search warrant, shall be fined under this title for a first offense; and, for a subsequent offense, shall be fined under this title or imprisoned not more than one year, or both.

Id.
to the warrant requirement for reasonable searches. Of utmost importance in this discussion is the border search exception.

C. Scope of the Border Search Exception

While the Fourth Amendment protects civilians from unreasonable searches and seizures by government officials, the Supreme Court has classified border zone searches as an exception to the warrant requirement. Border agents do not need warrants nor probable cause for basic border searches because the government has

26 See WARRANTLESS SEARCHES AND SEIZURES, supra note 24, at 40 (explaining that certain types of searches and seizures are valid as exceptions to the warrant requirement). [C]ertain kinds of searches and seizures are valid as exceptions to the probable cause and warrant requirements, including investigatory stops, investigatory detentions of property, warrantless arrests, searches incident to a valid arrest, seizures of items in plain view, searches and seizures justified by exigent circumstances, consent searches, searches of vehicles, searches of containers, inventory searches, border searches, searches at sea, administrative searches, and searches in which the special needs of law enforcement make the probable cause and warrant requirements impracticable.


27 See WARRANTLESS SEARCHES AND SEIZURES, supra note 24, at 108-09 (explaining border search exception). “Under the ‘border search’ exception to the warrant requirement, routine border stops and searches of persons, luggage, personal effects, and vehicles may be conducted without probable cause or reasonable articulable suspicion.” Id. See also J. Alan Boch, Validity of border searches and seizures by customs officers, 6. A.L.R. Fed. 317 (2022) (explaining that courts have held that one’s entry into the United States alone provides probable cause to search him/her); United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) (reasoning that government has a significant interest in searching people and goods entering the country, and therefore, reasonableness analysis is different at the border); United States v. Ramsey, 431 U.S. 606, 624–25 (1977) (holding that mail can be searched at border without warrant, probable cause, or reasonable suspicion).

28 See Boch, supra note 27 (explaining that the border search exception “permits a government officer at an international border to conduct a routine search and seizure, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into the United States.”); ANNE TOOMEY MCKENNA & CLIFFORD S. FISCHMAN, § 23:19. BORDER SEARCHES (2023) (detailing border search exception); United States v. Romm, 455 F.3d 990, 996 (9th Cir. 2006) (defining border search exception); United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006) (acknowledging border search exception); Montoya de Hernandez, 473 U.S. at 538 (explaining border search exception); Ramsey, 431 U.S. at 619 (detailing rationale behind the border exception).
a significant interest in protecting the country by examining the people and items entering it.\textsuperscript{29} More specifically, since border officials have a substantial interest in preventing the influx of contraband into the country, they can bypass the warrant requirement for searches.\textsuperscript{30} The Supreme Court has stated, “[b]order searches, then, from before the adoption of the Fourth Amendment, have been considered to be ‘reasonable’ by the single fact that the person or item in question had entered into our country from outside.”\textsuperscript{31}

The border search exception applies to searches by government officials within border zones, including international terminals for inbound flights at airports.\textsuperscript{32} Border agents can search one’s person and any items they seek to bring into the United States without a

\textsuperscript{29} See WARRANTLESS SEARCHES AND SEIZURES, supra note 24, at 119 (explaining rationale behind the border exception). “The Fourth Amendment does not require warrants for routine stops and searches at borders because the sovereign state and its public officials have the right to protect the United States by stopping and examining persons and property entering or leaving the country.” Id. at 108–09. See also United States v. Flores-Montano, 541 U.S. 149, 152 (2004) (indicating that “[g]overnment’s interest in preventing entry of unwanted persons and effects is at its zenith at international border.”); Montoya de Hernandez, 473 U.S. at 538 (discussing that government has power to protect the nation by examining persons entering the country); Ramsey, 431 U.S. at 619 (explaining that border searches are reasonable by single fact that the person or item had entered the country from outside). See also Claudia G. Catalano, Border Search or Seizure of Traveler’s Laptop Computer, or Other Personal Electronic or Digital Storage Device, 45 A.L.R. Fed. 2d 1 (2010) (detailing that basic border searches do not require a warrant or reasonable suspicion).

\textsuperscript{30} See Flores-Montano, 541 U.S. at 153 (emphasizing government’s interest in preventing the entry of contraband); Bradley v. United States, 299 F.3d 197, 202 (3d. Cir. 2002) (discussing custom officials’ substantial interest in preventing entry of narcotics into country); Montoya de Hernandez, 473 U.S. at 538 (explaining government’s interest in examining people and goods entering the country).

\textsuperscript{31} See Ramsey, 431 U.S. at 619 (justifying border searches on public safety principles). See also Flores-Montano, 541 U.S. at 152 (stressing the government’s interest in protecting international borders); Montoya de Hernandez, 473 U.S. at 538 (analyzing the government has power to examine entrants into this country).

\textsuperscript{32} See WARRANTLESS SEARCHES AND SEIZURES, supra note 24, at 119 (emphasizing the Fourth Amendment’s lack of a warrant requirement for routine stops and searches at borders . . . .’); Fox 5 Digital DC Team, supra note 1 (noting that border officials do not need a warrant or probable cause to search an arriving international traveler’s electronics); United States v. Arnold, 533 F.3d 1003, 1006 (9th Cir. 2008) (indicating that customs agents can search international travelers because a terminal is equivalent of international border); Bradley, 299 F.3d at 202 (discussing that customs agents can search international travelers because airports are equivalent to international borders and narcotics smuggling is a national crisis); Torres v. Commonwealth of P.R., 442 U.S. 465, 472–73 (1979) (explaining that United States has authority to search arriving international travelers’ baggage).
warrant or probable cause. The class of persons and items that border officials may search, however, is not limited to international travelers and their luggage. It also includes workers in border zones, persons engaged in suspicious behavior in a border zone, and vehicles. Furthermore, border officials can search items entering the country on their own, such as mail.

Although the usual restrictions on searches and seizures are relaxed in border zones, the search must still be reasonable by Fourth Amendment standards. Therefore, the totality of the circumstances must be considered when determining the constitutionality of warrantless border searches. Basic border searches, a pat down search for example, do not require reasonable suspicion. Since an extended, advanced border search entails greater delay than a basic border search, and thus a greater level of intrusion on reasonable expectations of privacy, government officials must justify the

33 See United States v. Barrow, 448 F.3d 37, 40–41 (1st Cir. 2006) (confirming that customs officials can search liquor bottles in border zones); United States v. Kelly, 302 F.3d 291, 293 (2002) (elucidating that one's person, including groin area, can be searched at international border by drug-sniffing dog); Torres, 442 U.S. at 472–73 (explaining that border agents can search arriving international travelers’ baggage “based on its inherent sovereign authority to protect its territorial integrity.”); Ramsey, 431 U.S. at 619 (explaining border agents’ practice of searching mail at international borders without warrant, probable cause, or reasonable suspicion).

34 See United States v. Glaziou, 402 F.2d 8, 13 (2d Cir. 1968) (discussing scope of persons and things subject to search by border officials).

35 See Glaziou, 402 F.2d at 13 (expanding upon the boundaries of the border search exception).

36 See Ramsey, 431 U.S at 624–25 (holding that agents can search mail at border without warrant, probable cause, or reasonable suspicion).

37 See Catalano, supra note 29 (explaining reasonableness requirement for border searches). “Although the usual restrictions on searches and seizures are relaxed at the border, such searches are governed by the reasonableness requirement of the Fourth Amendment.” Id.

38 See Catalano, supra note 29 (discussing that totality of the circumstances must be considered when determining constitutionality of a border search). “Thus, the totality of the circumstances must be taken into account in determining the legality of a stop and search by border patrol agents.” Id.

39 See Catalano, supra note 29 (emphasizing that basic border searches do not require any level of suspicion). “Under the border search doctrine, which creates an exception to the warrant requirement of the Fourth Amendment, a governmental official at an international border may conduct routine stops and searches without a warrant or probable cause.” Id.
extended search with reasonable suspicion that the search may reveal contraband.  

Travelers who have contested warrantless searches of their electronics in border zones have been largely unsuccessful. Most courts have held that the electronics search did not require reasonable suspicion of criminal activity per the border exception, or that officers had reasonable suspicion to conduct the search, or both. Furthermore, most courts found searches and seizures of electronics at international airport terminals specifically to be reasonable under the border search exception.

D. Recent Restrictions Established by the Supreme Court for Warrantless Searches of Electronics, and How They Affect International Travelers

In general, the Supreme Court has limited the scope of warrantless electronics searches. In *Riley v. California*, the Court held that warrantless searches of cell phones are generally

---

40 See Catalano, *supra* note 29 (explaining factors to consider when determining if an extended border search was reasonable). “Because the delayed nature of an extended border search necessarily entails a greater level of intrusion on legitimate expectations of privacy than an ordinary border search, the government must justify an extended border search with reasonable suspicion that the search may uncover contraband or evidence of criminal activity.” Id.

41 See Catalano, *supra* note 29 (acknowledging challenges faced by travelers who challenge constitutionality of border searches). “Travelers who have challenged the reasonableness of the warrantless search of their laptop computers, external hard drives, and other storage devices at border checkpoints have been largely unsuccessful.” Id.

42 See Catalano, *supra* note 29 (justifying why many courts have ruled against travelers challenging searches of their electronic devices in border zones); United States v. Ickes, 393 F.3d 501, 505 (4th Cir. 2005) (holding that search of a traveler’s computer and disks did not require reasonable suspicion).

43 See Arnold, 533 F.3d at 1008 (holding that search of a traveler’s laptop did not require reasonable suspicion under border exception); United States v. Romm, 455 F.3d 990, 996 (9th Cir. 2006) (holding that warrantless search of a traveler’s laptop was permissible without probable cause under border search exception); United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006) (holding that search of a traveler’s diskettes found in his luggage was supported by reasonable suspicion).

44 See, e.g., Carpenter v. United States, 138 S. Ct. 2206, 2210–11 (2018) (holding that the government must generally obtain a search warrant supported by probable cause before acquiring CSLI from a wireless carrier); Riley v. Cal., 573 U.S. 373, 376 (2014) (holding that warrantless search and seizure of cell phones is unconstitutional).
In that case, a search of the cell phone incident to arrest did not preclude the unconstitutionality of the search. In *Carpenter v. United States*, the Court held that the government must generally obtain a search warrant supported by probable cause before acquiring cell site location information (CSLI) from a wireless carrier. Courts have so far refused to enforce these restrictions on electronics searches in border zones. Unfortunately, this refusal has left international travelers exposed to the possibility that their sensitive, confidential information may be exposed.

Courts’ application of the border search exception to searches of electronic devices particularly affects professionals, such as lawyers, who carry confidential information on electronic devices.

---

45 See *Riley*, 573 U.S. at 376 (interpreting the Constitution as forbidding warrantless search and seizure of cell phones).
46 See *id.* at 373 (holding that the search incident to arrest does not justify a warrantless search of a cell phone).
47 See *Carpenter*, 138 S. Ct at 2210–11 (holding that searching CSLI from a wireless carrier generally requires a warrant supported by probable cause).
48 See, e.g., *Arnold*, 533 F.3d at 1008 (holding that searching a traveler’s laptop did not require reasonable suspicion); *Romn*, 455 F.3d at 1006 (holding that agents can search a traveler’s laptop without probable cause under the border search exception); *Irving*, 452 F.3d at 125 (holding that search reasonable suspicion was sufficient for search of a traveler’s diskettes). See also *Riley*, 573 U.S. at 402 (explaining that other exceptions to warrant requirement besides search incident to arrest exception, such as exigent circumstances exception, may justify warrantless searches of cell phones). “The critical point is that, unlike the search incident to arrest exception, the exigent circumstances exception requires a court to examine whether an emergency justified a warrantless search in each particular case.” *Id.*
49 See Jennifer Freeland et al., *Think Before You Pack that Laptop—Searches at the U.S. Border May Compromise Personal and Corporate Data*, VINSON & EILKINS (Feb. 18, 2021), archived at https://perma.cc/5QCH-8BQQ (highlighting data privacy concerns for companies and international travelers); Esha Bhandari et al., *Can Border Agents Search Your Electronic Devices? It’s Complicated.*, ACLU (Jan. 9, 2018) [hereinafter *Can Border Agents Search Your Devices?*], archived at https://perma.cc/B6HV-3G4K (discussing the ACLU’s opposition to the border search exception because of the private nature of material found on personal electronic devices); *Protecting Client Data*, supra note 1 (discussing concerns regarding the potential exposure of confidential client information during electronics searches at the border).
50 See Robert, supra note 11 (addressing concerns over breaches of attorney-client privilege during border searches); Lazzarotti & Atrakchi, *supra* note 11 (discussing issues for lawyers during border searches); Letter from Linda A. Klein, President of the A.B.A., to Gen. John F. Kelly, USMC (Ret.), See’y of Homeland Sec., and Joseph B. Maher, Acting Gen. Couns., Dept of Homeland Sec. (May 5, 2017) [on file with author] (expressing concern over ambiguity of CBP and ICE directives regarding searches of lawyers’ electronic devices that may result in breaches of privileged information).
The U.S. Customs and Border Patrol (“CBP”) maintains the authority
to read any document carried by a traveler, including documents found
on electronic devices, despite claims that such documents hold
attorney-client privileged information.\textsuperscript{51}

The American Bar Association (ABA) recently raised concern
over the rise of invasive electronics searches conducted by customs
agents in border zones.\textsuperscript{52} After expressing legitimate concerns
regarding “the standards that permit [the CBP] and Immigration and
Customs Enforcement (“ICE”) officers to search and review the
content of lawyers’ laptop computers, cell phones, and other electronic
devices at U.S. border crossings . . . ”, then-ABA President Linda Klein
requested several changes to CBP and ICE directives.\textsuperscript{53} President
Klein wrote, “first, we urge you to modify and clarify the [CBP and
ICE directives] to emphasize and protect these fundamental legal
rights and provide your front line agents and officers with explicit
guidance as to the importance of these principles.”\textsuperscript{54} Furthermore, she
wrote that the CBP and ICE directives “should specifically state that
the privileged or confidential electronic documents and files on the
device cannot be read, duplicated, seized, or shared unless the CBP
Officer or ICE Special Agent first obtains a subpoena based on
reasonable suspicion or a warrant supported by probable cause.”\textsuperscript{55}
Finally, she wrote, “[W]e recommend that DHS clarify [the CBP and
ICE directives] to:

\textsuperscript{51} See Lazzarotti & Atrakchi, supra note 11 (discussing CBP’s authority to read
information on lawyers’ electronic devices).
\textsuperscript{52} See Robert, supra note 11 (addressing concerns over breaches of attorney-client
privilege during border searches); Lazzarotti & Atrakchi, supra note 11 (discussing
concerns for lawyers during border searches); Klein, supra note 50 (expressing
concern over breaches of attorney-client privilege during searches of lawyers’
electronics).
\textsuperscript{53} See Klein, supra note 50 (requesting changes to CBP and ICE directives and
emphasizing importance of attorney-client privilege).
\textsuperscript{54} See Klein, supra note 50 (requesting additional guidance and protection for
attorneys against border searches of electronics). See also Robert, supra note 11
(detailing how border searches can lead to breaches of attorney-client privilege);
Lazzarotti & Atrakchi, supra note 11 (discussing concerns for lawyers during border
searches).
\textsuperscript{55} See Klein, supra note 50 (specifying that sensitive client information should not
be available for border agents to review). See also Robert, supra note 11 (discussing
how attorney-client privilege may be compromised during these searches);
Lazzarotti & Atrakchi, supra note 11 (expanding upon concerns for lawyers during
border searches).
(1) provide a clear standard that a CBP Officer or ICE Special Agent must follow prior to demanding a search or seizure of the documents and files on a lawyer’s electronic device;

(2) indicate what conduct is expected of the CBP Officer or ICE Special Agent when a lawyer asserts that an electronic device contains confidential client information protected under the attorney-client privilege, the work product doctrine, or the applicable rules of professional conduct; and

(3) define specifically when the CBP Officer or ICE Special Agent must consult with the CBP Associate/Assistant Chief Counsel, the ICE Office of the Chief Counsel, or the U.S. Attorney’s Office, including a specific requirement that the officer or agent do so whenever a lawyer asserts that an electronic device contains privileged or confidential client information and the officer or agent continues to seek access to that information.56

I. Facts

A. Recent Federal Jurisprudence Relating to Searches of Electronics

In recent years, the Supreme Court has declined to permit certain warrantless searches of electronic devices under established warrant requirement exceptions.57 In Riley v. California, the Court analyzed warrantless searches of cell phone data, which “marks a

56 See Klein, supra note 50 (requesting further protections when lawyers assert that an electronic device contains sensitive client information.) See also Robert, supra note 11 (addressing concerns over leaks of sensitive client information during these searches); Lazzarotti & Atrakchi, supra note 11 (explaining how these searches may subject attorneys to breaches of attorney-client privilege).

57 See Carpenter, 138 S. Ct at 2210–11 (2018) (holding that the agents can only review CSLI from wireless carriers after obtaining a search warrant supported by probable cause); Riley, 573 U.S. at 376 (2014) (holding that border agents cannot conduct warrantless search and seizure of cell phones).
turning point” in the Court’s jurisprudence regarding Fourth Amendment searches of electronic devices.\textsuperscript{58}

1. Riley v. California (Supreme Court of the United States, 2014)

Officers pulled over petitioner David Riley because his vehicle had expired registration tags and learned that Riley’s driver’s license was suspended.\textsuperscript{59} A search of the car revealed two handguns in the vehicle’s hood and officers arrested Riley for possession of concealed and loaded firearms.\textsuperscript{60} While searching Riley’s smartphone, officers discovered incriminating evidence that implicated Riley in a different incident.\textsuperscript{61} Using the evidence obtained from this search, the state charged Riley with firing at an occupied vehicle, assault with a semiautomatic firearm, and attempted murder.\textsuperscript{62} Riley moved to suppress the evidence as a violation of his Fourth Amendment rights.\textsuperscript{63}

The Court held that officers must generally obtain a warrant before conducting searches of cell phones.\textsuperscript{64} In justifying its holding, the Court first emphasized that cell phones possess an “immense

\textsuperscript{58} See Sean O’Grady, ALL WATCHED OVER BY MACHINES OF LOVING GRACE: BORDER SEARCHES OF ELECTRONIC DEVICES IN THE DIGITAL AGE, 87 FORDHAM L. REV. 2255, 2271 (2019) (discussing the Court’s new approach towards searches of electronic devices). “The Riley Court concluded that the traditional search-incident-to-arrest exception did not justify dispensing with the warrant requirement for searches of digital devices under the usual concerns for officers' safety or a fear of destruction of evidence.” Id. See also Riley, 573 U.S. at 386 (acknowledging the new approach taken by the Court by failing to extend existing precedent). “We therefore decline to extend Robinson to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search.” Id.

\textsuperscript{59} See Riley, 573 U.S. at 378 (detailing the initial reason that officers stopped Riley).

\textsuperscript{60} See id. (detailing why officers initially arrested Riley).

\textsuperscript{61} See id. at 379 (listing the incriminating evidence discovered by officers during search of Riley’s cell phone). “The officer accessed information on the phone and noticed that some words (presumably in text messages or a contacts list) were preceded by the letters ‘CK’—a label that, he believed, stood for ‘Crip Killers,’ a slang term for members of the Bloods gang.” Id. “Although there was ‘a lot of stuff’ on the phone, particular files that ‘caught [the detective's] eye’ included videos of young men sparring while someone yelled encouragement using the moniker ‘Blood.’” Id. “The police also found photographs of Riley standing in front of a car they suspected had been involved in a shooting a few weeks earlier.” Id.

\textsuperscript{62} See id. at 379 (2014) (summarizing state’s charges against Riley).

\textsuperscript{63} See id. (explaining Riley’s course of action after being charged by the state).

\textsuperscript{64} See id. at 386 (holding that officers must generally obtain a warrant prior to searching one’s cell phone).
storage capacity.” The capacity to store substantial amounts of personal information increases the potential for intrusions upon reasonable expectations of privacy during these searches. Furthermore, the Court reasoned that the information stored on cell phones is “quantitively different” than information that can be discovered on one’s person during a physical search. Chief Justice Roberts, writing for the majority, noted that cell phone data can reveal a person’s private interests or concerns, past location history, political views, habits, religious practices, and romantic life. Essentially, this information “can form a revealing montage of the user's life.” Finally, the Court noted the “pervasiveness” of cell phones in contemporary culture and the stark difference between routinely allowing police to access cell phone data as opposed to allowing them to access items obtained during a physical search. Courts have yet to apply the reasoning in Riley to searches of electronic devices in border zones. Furthermore, the Circuits currently disagree on the requirements for searching a traveler’s electronic devices.

65 See Riley, 573 U.S. at 393 (discussing the immense storage capacity of modern cell phones).
66 See id. (reasoning that potential for intrusions on privacy is amplified during searches of cell phones due to the sheer amount of information capable of being stored on them).
67 See id. at 395 (emphasizing that cell phone data reveals different aspects of one’s life than a physical search could).
68 See id. at 395–96 (expounding upon the different types of information that can be found during a search of one’s cell phone).
69 See id. at 396 (highlighting the differences between conducting searches of cell phones and other items).
70 See id. at 395 (discussing the pervasiveness of cell phones in the modern age).
71 Compare Riley, 573 U.S. at 386 (holding that officers must generally obtain a warrant prior to searching one’s cell phone), with Alasaad, 988 F.3d at 18 (holding that customs agents can perform basic electronics searches without suspicion), Kolsuz, 890 F.3d at 144, 148 (holding that smartphone searches are nonroutine, and therefore, customs agents need reasonable suspicion to conduct a smartphone search), and Touset, 890 F.3d at 1232 (holding that customs agents do not need any level of suspicion to conduct searches of electronic devices).
72 Compare Kolsuz, 890 F.3d at 144, 148 (holding that customs agents in Fourth circuit territory need reasonable suspicion to conduct forensic searches of electronic devices), with Touset, 890 F.3d at 1232 (holding that customs agents in Eleventh Circuit territory do not need any level of suspicion prior to conducting a search travelers’ electronics).
2. *Alasaad v. Mayorkas* (First Circuit, 2021)

In this case, numerous plaintiffs sought to enjoin current CBP and ICE policies. They contested policies allowing border agents to perform basic electronics searches without reasonable suspicion, advanced electronics searches with only reasonable suspicion, and searches unrelated to contraband. They argued that all electronic device searches at the border should require a warrant, or in the alternative, that they should require reasonable suspicion of evidence of contraband being found on the device.

The First Circuit held that border agents need not secure a warrant prior to conducting an electronics search. They explained that *Riley* did not establish a categorical rule requiring agents to secure a warrant prior to such searches. Furthermore, the court reasoned that the immense volume of international travelers crossing into the
United States requires border agents to conduct warrantless border searches as a protective measure.\(^78\)

The court then held that basic border searches do not require any level of individualized suspicion prior to conducting the search.\(^79\) It reasoned that searches of electronic devices do not involve intrusive searches of one’s person.\(^80\) Furthermore, basic electronics searches require an officer to manually traverse the device’s contents, thus limiting the quantity of information available during the search.\(^81\)

Finally, the court held that border agents need not limit the scope of electronics searches to investigations into contraband.\(^82\) The court reasoned that warrantless searches must be justified by the particular purposes of the exception that allows it.\(^83\) Since the

\(^{78}\) See id. at 17 (justifying warrantless searches at the border due to the immense volume of international travelers crossing into the United States). “[A] warrant requirement -- and the delays it would incur -- would hamstring the agencies' efforts to prevent border-related crime and protect this country from national security threats.” Id.

\(^{79}\) See Alasaad, 988 F.3d at 18 (holding that border agents may perform routine searches without reasonable suspicion). Additionally, the court explained that non-routine searches must be grounded in reasonable suspicion. Id. Whether a border search is routine or non-routine depends on the totality of the circumstances. Id.

\(^{80}\) See id. (reasoning that an electronics search is routine, and thus does not require reasonable suspicion, because it does not involve an invasive search of one’s person). The court begins by reasoning that electronic devices “implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.” Id. (quoting Riley, 573 U.S. at 393). However, these concerns are “tempered by the fact that the searches occur at the border, where the ‘[g]overnment's interest in preventing the entry of unwanted persons and effects is at its zenith.’” Id. (quoting Flores-Montano, 541 U.S. at 152). The court then lists two justifications for these border searches, including that they do not violate one’s person. Id.

\(^{81}\) See id. (reasoning that the amount of information available to agents during a basic electronics search is limited by the nature of the search). “The CBP Policy only allows searches of data resident on the device.” Id. at 18–19 (citing CBP POLICIES, supra note 5, at 4). “And a basic border search does not allow government officials to view deleted or encrypted files.” Id. at 19.

\(^{82}\) See id. at 19 (holding the scope of border searches of electronic devices need not be limited to searches for contraband). Plaintiffs argued that these searches must be limited in scope to searches for contraband because the border search exception only seeks to prevent the importation of contraband or inadmissible persons, and covers only searches for contraband itself, rather than evidence of crimes or contraband. Id.

\(^{83}\) See id. (citing Florida v. Royer, 460 U.S. 491, 500 (1983)) (discussing that warrantless searches “must be limited in scope to that which is justified by the particular purposes served by the exception.”).

\textit{Riley} did not purport to extend [its holding] to the border search context. Even assuming arguendo that the analysis used in \textit{Riley} applies here, such an analysis would only require that warrantless
government’s interest in preventing crime “is at its zenith” at the borders, and searches related to general cross-border crime serve this purpose, border searches need not be limited to searches for contraband.  


In this case, customs agents detained petitioner Hamza Kolsuz, while he attempted to board a flight to Turkey, after discovering firearms parts in his luggage. Customs agents arrested Kolsuz and seized his smartphone prior to conducting an off-site forensic analysis of its contents. Kolsuz moved to suppress evidence from the search because it violated his Fourth Amendment rights. The District Court denied the motion, holding that the border search exception applied and the forensic analysis of the phone constituted a nonroutine search justified by reasonable suspicion.

> border searches be tethered to “the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country.”

*Id.* (quoting *Ramsey*, 541 U.S. at 152).

84 See *id.* at 19 (discussing the court’s reasoning for its holding). The court first reasoned, warrantless routine searches without reasonable suspicion “are reasonable simply by virtue of the fact that they occur at the border.” *Id.* (quoting *Ramsey*, 431 U.S. at 616). “This is . . . because the 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 to the warrant requirement.” *Id.* (quoting *Flores-Montano*, 541 U.S. at 152).

85 See *Kolsuz*, 890 F.3d at 136 (detailing the initial encounter between petitioner and custom agents that led to the search in question).

86 See *id.* (explaining that customs agents seized the phone and conducted an off-site forensic analysis of its contents). “After arresting Kolsuz, the agents took possession of his smartphone and subjected it to a month-long, off-site forensic analysis, yielding a nearly 900-page report cataloguing the phone's data.” *Id.* The court acknowledged the “temporal and spatial distance” between the phone’s initial seizure and the off-site search but held that the border search exception is broad enough to cover that off-site search. *Id.* at 137.

87 See *id.* at 139–40 (discussing petitioner’s motion to suppress the evidence obtained from the forensic search). “According to Kolsuz, a forensic search of a phone that occurs miles away from an airport and for a month after an attempted departure does not constitute a ‘border search.’” *Id.* “Instead, Kolsuz argued, the forensic search should be treated as a search incident to his arrest, and under *Riley v. California*, cell phones may be searched incident to arrest only with a warrant based on probable cause.” *Id.* at 140.

88 See *id.* at 140 (describing the court’s reasoning for denying petitioner’s motion to suppress). “The court held first that the forensic search of Kolsuz's phone was
The Fourth Circuit first held that a forensic search of a smartphone is a nonroutine, advanced search. It reasoned that the “sheer quantity of data stored on smartphones and other digital devices” exceeds the amount of personal information that one could personally carry over the border. Furthermore, the “sensitive nature” of the data and the ubiquitous nature of smartphones in the modern world implicates more significant privacy concerns. Finally, the court held that nonroutine, advanced border searches require reasonable suspicion. It cited court precedent and recent developments that called for reasonable suspicion in these cases, and not a warrant supported by probable cause, as Kolsuz argued.


After an extensive investigation by several entities into petitioner Touset’s potential involvement with child pornography, customs agents detained him after he arrived in Atlanta, Georgia on an international flight. Agents manually searched petitioner’s two properly evaluated as a border search. That Kolsuz had been arrested, the district court explained, did not transform the forensic examination into a search incident to arrest or render the border exception inapplicable . . . .” *Id.* (citing *Ickes*, 393 F.3d at 507). The court then reasoned that it is difficult to think of a search more personally invasive than an advanced search of one’s smartphone, and therefore, the forensic search of the phone was nonroutine. *Id.* Finally, the court cited precedent in holding that nonroutine border searches require reasonable suspicion. *Id.*

89 See *id*. at 144 (holding that forensic searches of smartphones are nonroutine). “[I]n deciding whether a search rises to the level of nonroutine, courts have focused primarily on how deeply it intrudes into a person's privacy.” *Id.* “Under that approach . . . searches that are most invasive of privacy—strip searches, alimentary-canal searches, x-rays, and the like—are deemed nonroutine . . . .” *Id.*

90 See *id*. at 145 (highlighting the immense storage capacity of smartphones as justification for why searches of smartphones are nonroutine).

91 See *Kolsuz*, 890 F.3d at 145 (reasoning that the uniquely sensitive nature of the information on electronic devices, and the ubiquitous nature of these devices in the modern world, support a conclusion that searches of these devices are nonroutine).

92 See *id*. at 146 (holding that nonroutine, forensic searches of cell phones “requir[e] some form of individualized suspicion.”).

93 See *id*. at 146 (reasoning that precedent and recent developments support the court’s holding). “After *Riley*, we think it is clear that a forensic search of a digital phone must be treated as a nonroutine border search, requiring some form of individualized suspicion.” *Id.* The majority also noted that the Department of Homeland Security established that forensic searches of digital devices are nonroutine shortly after oral arguments for this case. *Id.* (citing U.S. CUSTOMS AND BORDER PROT., CBP DIRECTIVE NO. 3340–049A, BORDER SEARCH OF ELECTRONIC DEVICES 5 (2018)).

94 See *Touset*, 890 F.3d at 1230 (describing the events leading to the search in question).
iPhones, and seized a camera, two laptops, two external hard drives, and two tablets for forensic examination.\textsuperscript{95} This analysis revealed child pornography.\textsuperscript{96} Eventually, a grand jury indicted petitioner on three counts related to child pornography.\textsuperscript{97} Petitioner moved to suppress the evidence.\textsuperscript{98}

The Eleventh Circuit held that customs agents do not need any level of suspicion to conduct a search of one’s electronic devices in border zones.\textsuperscript{99} The court reasoned that while the Supreme Court has mandated a showing of reasonable suspicion before conducting nonroutine, advanced searches of persons, it has never extended this requirement to searches of property.\textsuperscript{100} Moreover, the court identified three factors that elevate the intrusiveness of a search—physical contact between the searcher and the person searched, exposure of intimate body parts, and use of force.\textsuperscript{101} The court explained that these factors do not apply to searches of electronic devices.\textsuperscript{102} Finally, the court reasoned that a traveler’s privacy interests should not be given

\textsuperscript{95} See id. (explaining that customs agents seized Touset’s electronic devices and forensic analysts conducted a forensic search of those devices).
\textsuperscript{96} See id. (detailing that forensic analysis “revealed child pornography on the two laptops and the two external hard drives.”).
\textsuperscript{97} See id. (describing the events that led to Touset’s indictment after agents discovered child pornography in his home).
\textsuperscript{98} See id. at 1231 (stating that Touset motioned to suppress evidence obtained from the search and the magistrate judge denied that motion).
\textsuperscript{99} See id. at 1233 (holding that customs agents do not need any level of suspicion to search electronic devices in a border zone).
\textsuperscript{100} See Touset, 890 F.3d at 1233 (elucidating that the Supreme Court has never extended the reasonable suspicion requirement to intrusive property searches). “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.” Id.
\textsuperscript{101} See id. at 1234 (discussing factors the court considers when analyzing the intrusiveness of a search). “In contrast with searches of property, we have required reasonable suspicion at the border only for highly intrusive searches of a person’s body.” Id. (citing United States v. Alfaro-Moncado, 607 F.3d 720, 729 (11th Cir. 2010)). “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. (quoting United States v. Vega-Barvo, 729 F.2d 1341, 1346 (11th Cir. 1984)).
\textsuperscript{102} See id. (explaining that these factors are irrelevant to searches of electronic devices). Id. “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.” Id.
greater weight than protecting the territorial integrity of the United States.\(^\text{103}\)

**B. The Current Situation for International Travelers**

The lack of agreement among the circuits regarding electronic device searches has striking implications for international travelers.\(^\text{104}\) All travelers risk exposing potentially sensitive information.\(^\text{105}\) Worse yet, recent developments have revealed that CBP agents consistently copy information discovered during these electronics searches and store it in an unregulated database to which all CBP agents have access.\(^\text{106}\) Depending on the airports at which travelers arrive, or

\(^{103}\) See id. at 1235 (weighing the importance of protecting the border against a traveler’s privacy interests). “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. (quoting Flores-Montano, 541 U.S. at 153).

\(^{104}\) See Dana Khazzaz, *How CBP Uses Hacking Technology to Search International Travelers’ Phones*, ELEC. PRIV. INFO. CTR. (Feb. 22, 2022), archived at https://perma.cc/74UY-J6Y3 (discussing the invasive nature of technology used by CBP to conduct electronics searches); Freil, *supra* note 49 (emphasizing the danger of privacy breaches for companies and international travelers). See also *Can Border Agents Search Your Devices?*, *supra* note 49 (discussing the ACLU’s opposition to the border search exception because electronic devices possess private, sensitive information).


which international border they intend to cross, travelers carry different privacy rights and risk exposure of sensitive information as a result.107

IV. Analysis

The First Circuit currently operates under the Alasaad framework which provides that basic electronic searches at the border do not require any level of suspicion, while advanced searches require reasonable suspicion but do not have to be limited in scope to searches for digital contraband. 108 The Fourth Circuit follows similar principles under the Kolsuz framework.109 The Eleventh Circuit, however, follows a contradictory approach under the Touset framework, which does not require any level of suspicion for electronics searches at the borders.110 To complicate things further, the Ninth Circuit limits the scope of any electronics searches to searches for digital contraband under the Cano framework.111

107 Compare Kolsuz, 890 F.3d at 146 (holding that customs agents in Fourth Circuit territory must have reasonable suspicion to forensically search electronic devices), with Touset, 890 F.3d at 1233 (holding that customs agents in Eleventh Circuit territory do not need any level of suspicion prior to conducting a search of one’s electronics, no matter how invasive), and Alasaad, 988 F.3d at 20 (holding that border searches in First Circuit Territory do not need to be limited in scope to searches for contraband).

108 See Alasaad, 988 F.3d at 19–20 (holding that customs agents need not have reasonable suspicion to conduct basic border searches or more advanced searches for contraband). See also Arnold, 533 F.3d at 1009–10 (holding that customs agents do not need reasonable suspicion to search laptops).

109 See Kolsuz, 890 F.3d at 137 (holding that customs agents do not need reasonable suspicion to conduct basic border searches).

110 See Touset, 890 F.3d at 1233 (holding that border searches need not be supported by reasonable suspicion). “We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device . . . .” Id. “[I]t 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 . . . .” Id.

111 See Cano, 934 F.3d at 1018 (holding that border searches in Ninth Circuit territory must be limited in scope to searches for contraband). “[W]e hold that the border search exception authorizes warrantless searches of a cell phone only to determine whether the phone contains contraband. A broader search cannot be ‘justified by the particular purposes served by the exception.’” Id.
The Circuits disagree regarding travelers’ privacy rights. This disagreement facilitates varying levels of constitutional protection, and thus disparities in treatment, depending on one’s location. For example, if an international traveler arrives at Miami International Airport, a customs agent could perform a thorough search of their electronic devices, and seize sensitive information for storage in federal databases, without possessing any suspicion that the traveler has committed a crime. If that same traveler, however, arrived at Daniel K. Inouye International Airport in Hawaii, a customs agent would need reasonable suspicion that the traveler has committed a crime prior to performing a thorough search of their electronic devices.

112 Compare *Alasaad*, 988 F.3d at 19–20 (deciding that border searches in First Circuit do not have to be limited in scope to searches for contraband); and *Kolsuz*, 890 F.3d at 142 (holding that border searches in Fourth Circuit are not limited in scope to searches for contraband); *with Cano*, 934 F.3d at 1018 (holding that border searches in Ninth Circuit must be limited in scope to searches for contraband). Compare *Kolsuz*, 890 F.3d at 146 (holding that nonroutine, forensic border searches require individualized suspicion); *with Touset*, 890 F.3d at 1233 (holding that agents do not need reasonable suspicion to perform any border search).

113 Compare *Alasaad*, 988 F.3d at 19–20 (deciding that border searches in First Circuit territory do not have to be limited in scope to searches for contraband), and *Kolsuz*, 890 F.3d at 142 (holding that border searches in Fourth Circuit territory are not limited in scope to searches for contraband), *with Cano*, 934 F.3d at 1018 (holding that border searches in Ninth Circuit territory must be limited in scope to searches for contraband). Compare *Kolsuz*, 890 F.3d at 146 (holding that nonroutine, forensic border searches in Fourth Circuit territory require individualized suspicion), *with Touset*, 890 F.3d at 1233 (holding that agents in Eleventh Circuit territory do not need reasonable suspicion to perform any border search). See also FOX 5 Digital DC Team, *supra* note 1 (highlighting that border officials at international airport terminals do not need a warrant or even probable cause to search one’s electronics); *Protecting Client Data*, *supra* note 1 (expressing concern over rise in searches of lawyers’ electronic devices in airports).

114 See *Touset*, 890 F.3d at 1233 (holding that customs agents in Eleventh Circuit territory, which includes Florida, do not need reasonable suspicion to perform any border search). See also FOX 5 Digital DC Team, *supra* note 1 (pointing out that border officials at international airport terminals do not even need probable cause to search travelers’ electronics); Kan, *supra* note 106 (discussing that CBP agents copy data from travelers’ phone without any reason and store it in an unregulated government database).
The importance of this crucial constitutional protection dictates a need for consistency among the circuits.\textsuperscript{115} The first and most aggressive approach involves applying the \textit{Riley} standard to electronic searches in border zones.\textsuperscript{117} In \textit{Riley}, the Court held that warrantless searches of cell phones are unconstitutional.\textsuperscript{118} Justice Roberts reasoned that the immense storage capacity of cell phones, the sensitive and personal nature of the data stored on cell phones, and the pervasiveness of cell phones in contemporary society increases the potential for intrusions upon

\textsuperscript{115} See \textit{Kolsuz}, 890 F.3d at 146 (holding that nonroutine, forensic border searches in Ninth Circuit territory, which includes Hawai'i, require individualized suspicion). \textit{See also FOX 5 Digital DC Team, supra note 1} (emphasizing the low standard of suspicion that customs agents must meet to conduct electronic searches).

\textsuperscript{116} See \textit{Can Border Agents Search your Devices?}, supra note 49 (arguing that constitutional safeguards established in \textit{Riley} should apply to all unwarranted searches of electronic devices at borders). "[T]here’s no reason the Constitution’s safeguards against unwarranted searches shouldn’t also apply when we travel internationally given the ubiquity of these devices, and their ever-growing capacity to track the minutiae of our private lives.” \textit{Id. See also Vernick & Monnin, supra note 105} (discussing an upcoming Eighth Circuit case regarding an unwarranted forensic search of a reporter’s electronic devices at O’Hare International Airport).

Authors discussed that the border search exception should not automatically apply to electronic device searches because this intrudes upon newsgathering and infringes upon Fourth Amendment rights of international travelers. \textit{Id. See generally Gina R. Bohannon, Cell Phones and the Border Search Exception: Circuits Split over the Line Between Sovereignty and Privacy, 78 MD. L.REV. 563, 603 (2019)} (concluding that establishing a warrant requirement for electronic device searches at the border is necessary due to the intrusiveness of these searches and tenuous justification by the border search exception). "As legal challenges to electronic device searches at the border continue to arise, courts should recognize their significant intrusion on individual privacy and tenuous relationship with the traditional justification for the border search exception.” \textit{Id. “[I]mposing a warrant requirement to search personal electronic devices at the border would avoid these problems and give clear guidance to law enforcement.” Id.}

\textsuperscript{117} See \textit{Riley}, 573 U.S. at 376 (holding that the warrantless search and seizure of cell phones is unconstitutional); Bohannon, \textit{supra} note 116, at 603 (advocating for a warrant requirement to perform electronic device searches at borders); \textit{Can Border Agents Search Your Devices?}, \textit{supra} note 49 (arguing that constitutional safeguards established in \textit{Riley} should apply to all unwarranted searches of electronic devices at borders). \textit{But see Alasaad, 988 F.3d at 17} (reasoning that the holding in \textit{Riley} does not extend to the present case). The First Circuit reasoned that not only does \textit{Riley} not establish a rule requiring warrants for electronic device searches, but it does not apply to border searches. \textit{See id.}

\textsuperscript{118} See \textit{Riley}, 573 U.S. at 376 (explaining the unconstitutionality of warrantless searches and seizures of cell phones). “[T]he Court's holding is not that the information on a cell phone is immune from search; it is that a warrant is generally required before a search.” \textit{Id.}
reasonable expectations of privacy during these searches. Courts have yet to extend the holding in Riley to border searches, and continue to justify warrantless searches of all electronic devices, including cell phones, under the border search exception.

That same reasoning used by Justice Roberts applies to electronic device searches in border zones. Cell phones, laptops, tablets, and smart watches do not lose the ability to retain massive

119 See id. at 375 (discussing the unique characteristics of cell phones that justify the holding).

Cell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person. Notably, modern cell phones have an immense storage capacity. Before cell phones, a search of a person was limited by physical realities and generally constituted only a narrow intrusion on privacy. But cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos. This has several interrelated privacy consequences. First, a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record. Second, the phone's capacity allows even just one type of information to convey far more than previously possible. Third, data on the phone can date back for years. In addition, an element of pervasiveness characterizes cell phones but not physical records.

Id.

120 See Alasaad, 988 F.3d at 17 (reasoning that the holding in Riley does not apply to this case). The First Circuit reasoned that not only does Riley not establish a rule requiring warrants for electronic device searches, but it does not apply to border searches. Id. See generally Kolsuz, 890 F.3d at 137 (holding that basic border searches do not require reasonable suspicion, and thus, do not require a warrant); Touset, 890 F.3d at 1233 (holding that electronic device searches at border do not require individualized suspicion, and thus, do not require a warrant).

121 See Can Border Agents Search Your Devices?, supra note 49 (arguing that constitutional safeguards established in Riley should apply to all unwarranted searches of electronic devices at borders). “[T]here’s no reason the Constitution’s safeguards against unwarranted searches shouldn’t also apply when we travel internationally given the ubiquity of these devices, and their ever-growing capacity to track the minutiae of our private lives.” Id. See also Vernick & Monnin, supra note 105 (discussing an upcoming Eighth Circuit case regarding an unwarranted forensic search of a reporter’s electronic devices at O’Hare International Airport). “[O]ur electronic devices hold vast troves of personal and expressive information providing an ‘intimate window into a person’s life,’ and such a search raises independent First Amendment concerns. A forensic search is extremely intrusive, allowing law enforcement to search through an exact replica of the contents of the device.” Id.
amounts of travelers’ sensitive, personal information at the border. Lawyers, specifically, store highly sensitive and confidential case information on personal electronic devices. Why, then, can customs agents rummage through these devices without a warrant indicating a legitimate reason to do so? Riley signaled an understanding that cell phone searches require a warrant due to certain characteristics that distinguish cell phone data searches from other searches, including their immense storage capacity, their ability to store sensitive information, and their ubiquity in modern society. All electronic devices should fall under this category considering they can also store vast amounts of highly sensitive information.

122 See Khabbaz, supra note 104 (discussing the invasive nature of technology used by CBP to conduct electronics searches). Khabbaz discusses that in contemporary society, people store intimate information on electronic devices such as cell phones. Id. Therefore, these warrantless searches of electronic devices in border zones are very intrusive. Id. See also Can Border Agents Search Your Devices?, supra note 49 (emphasizing that the “ubiquity” of electronic devices and “their ever-growing capacity to track the minutiae of our private lives” dictates a need for increased privacy protections).

123 See Protecting Client Data, supra note 1 (expressing concern over rise in searches of lawyers’ electronic devices and discussing how to protect against confidentiality breaches). The article discusses that given the current situation, attorneys must remain vigilant of the possibility of a customs agent searching electronic devices containing privileged information. Id. Furthermore, attorneys must take reasonable precautions to guard against this information being discovered during a search and must inform the client if a device containing privileged information is searched or seized. Id. See also Robert, supra note 11 (addressing concerns over breaches of attorney-client privilege during border searches). See generally Freel, supra note 49 (highlighting data privacy concerns for companies and international travelers). “In an increasingly interconnected global economy, employees often travel with confidential, privileged, personal, or proprietary data on their electronic devices.” Id.

124 See Can Border Agents Search Your Devices?, supra note 49 (arguing that measures established in Riley should also apply to border searches of electronics). Bhandari argues that the Constitution’s protections against unwarranted searches should apply to international travelers in border zones given the pervasiveness of these devices, and their capacity to store immense amounts of personal, sensitive information. Id.

125 See Riley, 573 U.S. at 393 (distinguishing searches of cell phone data from physical searches because of a cell phone’s immense storage capacity, ability to store sensitive information, and the ubiquity of cell phones).

126 See Can Border Agents Search Your Devices?, supra note 49 (reasoning that measures established in Riley should apply to all unwarranted searches of electronic devices at borders). “[T]here’s no reason the Constitution’s safeguards against unwarranted searches shouldn’t also apply when we travel internationally given the ubiquity of these devices, and their ever-growing capacity to track the minutiae of
counterargument to this proposition would likely revolve around common justifications for the border search exception.\textsuperscript{127} Essentially, these arguments boil down to the government having a duty to ensure that unwanted persons and items do not cross the border.\textsuperscript{128}

An alternative to the warrant requirement involves classifying all electronic device searches as nonroutine, advanced searches, and thus, requiring customs agents to have individualized suspicion of criminal activity prior to conducting these searches.\textsuperscript{129} Furthermore, our private lives.” \textit{See also} Khabbaz, \textit{supra} note 104 (emphasizing how invasive electronics searches by CBP officials can be). Due to the tendency to store large amounts of personal information on electronic devices, these searches can be very invasive. \textit{Id.}  

\textsuperscript{127} \textit{See} Bohannon, \textit{supra} note 116, at 570–71 (discussing historical justifications for the border search exception).

Historically, border searches have been deemed reasonable without a warrant because of the compelling government interest in controlling who and what may cross into the nation's sovereign territory. The Constitution gives the federal government various specific powers that require oversight of what persons and property cross the border, including the power to “provide for the common defence,” “regulate commerce with foreign nations,” and “establish a uniform rule of naturalization.” \textit{Id.} \textit{See also} WARRANTLESS SEARCHES AND SEIZURES, \textit{supra} note 24, at 120–21 (explaining that the Fourth Amendment does not mandate warrants for routine searches at borders because the government has the right to protect the country by examining persons and property crossing the border). \textit{See also} Arnold, 533 F.3d at 1006 (discussing that customs agents can search international travelers because terminal is equivalent of international border); \textit{Bradley}, 299 F.3d at 202 (stating that customs agents can search international travelers because airports are equivalent to international borders and narcotics smuggling is a national crisis); \textit{Kelly}, 302 F.3d at 294 (indicating that one’s person, including groin area, can be searched at international border by drug-sniffing dog). \textit{See generally} Touset, 890 F.3d at 1232 (relating the Framers’ intent to moderate justifications for the border search exception). “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.” \textit{Id.}

\textsuperscript{128} \textit{See} Bohannon, \textit{supra} note 116, at 570–71 (discussing the compelling government interest to facilitate who and what comes into the country). Bohannon also writes about constitutional arguments justifying the border search exception, including “‘prov[iden]ce,’ ‘regulat[ing] commerce with foreign nations,’ and ‘establish[ing] an uniform rule of naturalization.’” \textit{Id.} \textit{See also} WARRANTLESS SEARCHES AND SEIZURES, \textit{supra} note 24, at 120–21 (emphasizing the government’s duty to protect the country by inspecting who and what crosses the border).

\textsuperscript{129} \textit{See} Kolsuz, 890 F.3d at 144–46 (holding that smartphone searches are nonroutine, and therefore, customs agents need reasonable suspicion to conduct them). \textit{But see}
these searches should be limited to searches for digital contraband. Requiring reasonable suspicion supports a strong likelihood that law-abiding citizens will not be subjected to searches of their electronic devices. Furthermore, this alternative would protect a traveler’s privacy by restricting the search, and thus, guarding against the discovery of personal, sensitive information unrelated to the suspicion. This solution protects the privacy interests of international travelers while also permitting customs agents to perform

\textit{Alasaad}, 988 F.3d at 18 (holding that customs agents can perform basic electronics searches without suspicion); \textit{Touset}, 890 F.3d at 1233 (holding that customs agents do not need any level of suspicion to conduct searches of electronic devices).\footnote{See \textit{Cano}, 934 F.3d at 1018 (holding that border searches in the Ninth Circuit must be limited in scope to searches for contraband). \textit{But see Alasaad}, 988 F.3d at 19 (deciding that border searches in the First Circuit need not be limited in scope to searches for contraband); \textit{Kolsuz}, 890 F.3d at 142 (holding that border searches in the Fourth Circuit are not limited in scope to searches for contraband).}

\textit{See Telvock}, supra note 1 (quoting Senator Ron Wyden, who urged the Commissioner of Customs and Border Protection to adopt more stringent search procedures). Sen. Wyden wrote to the Commissioner, “I urge you to update Customs and Border Protection’s practices regarding searches of Americans’ phones and electronic devices at the border to focus on suspected criminals and security threats, rather than allowing indiscriminate rifling through Americans’ private records without suspicion of a crime . . . .” (emphasis added). \textit{Id.} The Electronic Frontier Foundation agreed with Sen. Wyden and emphasized that indiscriminate electronic device searches “pose a grave threat to civil liberties and chills First Amendment-protected activities.” \textit{Id.} EFF went on to say, “[w]e believe that the Fourth Amendment absolutely should apply at the border . . . [t]he exception cannot be so broad as to allow essentially a fishing expedition by the government.” \textit{Id.} \textit{See also Lazzarotti \\& Atrakchi}, supra note 11 (indicating the problems encountered by attorneys when customs agents search work devices that contain privileged information). “For lawyers, invasive CBP searches are particularly problematic, as the CBP asserts that it has the authority to read any document in possession of a traveler, including those found on electronic devices, despite claims that such documents are attorney-client privileged information.” \textit{Id.} The ABA has, and continues to, seek more stringent search policies to protect against breaches of confidential attorney-client information. \textit{Id.} \footnote{See Lazzarotti \\& Atrakchi, supra note 11 (identifying the issues attorneys face when customs agents search work devices that contain privileged information). In 2017, the DHS, working closely with the ABA, modified the CBP’s electronic device search directive as it applies to attorneys. \textit{Id.} Important changes to the directive included, “a requirement for CBP officers to consult with CBP’s senior counsel before searching devices when an attorney client privilege is asserted; details for how CBP officers should respond to such assertions; segregation of privileged material; and disposal of privileged materials.” \textit{Id.} \textit{See also Robert}, supra note 11 (discussing a resolution passed by the ABA House of Delegates that the federal judiciary, Congress, and Homeland Security should protect against breaches of attorney-client privilege during searches of electronic devices in border zones).}
these searches without the hassle of obtaining a warrant.\textsuperscript{133} One may counter this solution by arguing that basic electronic searches already require manually traversing through electronic devices.\textsuperscript{134} Therefore, this practical constraint sufficiently limits the scope of the search and protects a traveler’s privacy, and customs agents should not also be required to develop reasonable suspicion prior to the search.\textsuperscript{135}

While this justification is debatable, considering that personal and sensitive information can be discovered during basic and advanced electronics searches, this constraint does not affect the need for all jurisdictions to require reasonable suspicion prior to advanced electronics searches.\textsuperscript{136} Advanced electronics searches occur at specially designed facilities and benefit from advanced, external technology designed to obtain and organize massive amounts of digital

\textsuperscript{133} See Can Border Agents Search Your Devices, supra note 49 (discussing the ACLU’s objections to current border search policies). “As the ACLU has argued in various court filings, there’s no reason the Constitution’s safeguards against unwarranted searches shouldn’t also apply when we travel internationally given the ubiquity of these devices, and their ever-growing capacity to track the minutiae of our private lives.” Id. See also Robert, supra note 11 (emphasizing the need for protecting against breaches of attorney-client privilege during border searches of electronic devices).

\textsuperscript{134} See Alasaad, 988 F.3d at 18 (emphasizing the manual nature of physically traversing through an electronic device).

\textsuperscript{135} See id. (discussing that the manual nature of basic electronic searches sufficiently limits the amount of information available to officers, and thus, sufficiently protects against intrusive discovery of sensitive information). “Basic border searches also require an officer to manually traverse the contents of the traveler's electronic device, limiting in practice the quantity of information available during a basic search.” Id.

\textsuperscript{136} See Kolsuz, 890 F.3d at 138 (identifying a category of “nonroutine” border searches that can only be performed if the customs agent has individualized suspicion the traveler is committing a crime) (citing Montoya de Hernandez, 473 U.S. at 541). “Such nonroutine border searches, the Court has suggested, include ‘highly intrusive searches’ that implicate especially significant ‘dignity and privacy interests,’ as well as destructive searches of property and searches carried out in ‘particularly offensive’ manners.” Id. (citing Flores-Montano, 541 U.S. at 152, 154). See also CBP Policies, supra note 5 (explaining the difference between advanced and basic electronics searches). “An advanced search is any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents.” Id. at 5. “Any border search of an electronic device that is not an advanced search . . . may be referred to as a basic search.” Id. at 4. See generally Telvock, supra note 1 (identifying the need for uniformity among the Circuits regarding how the border search exception is applied by customs agents). “[T]he highest court in the land will eventually have to chime in to remove any doubt on how the exception gets applied by international border agents.” Id.
information. The likelihood of agents discovering sensitive, personal, confidential information during advanced searches is much greater than during basic searches. For example, an advanced search of an attorney’s laptop could easily grant access to thousands of pages of privileged documents related to pending cases, in violation of attorney-client privilege and confidentiality. Therefore, agents should be required to have reasonable suspicion of criminal activity related to the device before performing these highly invasive searches.

See CBP Policies, supra note 5, at 4–5 (distinguishing advanced and basic border searches). “An advanced search is any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents.” Id. at 5. See also Kolsuz, 890 F.3d at 145 (pointing to Riley and explaining that forensic searches of electronic devices are considered “nonroutine” because of the immense quantity of data stored on these devices, the sensitive nature of that data, and the ubiquity of these devices). “After Riley, we think it is clear that a forensic search of a digital phone must be treated as a nonroutine border search, requiring some form of individualized suspicion.” Id. at 146.

See CBP Policies, supra note 5, at 4–5 (distinguishing between advanced electronic device searches and basic electronic device searches). During advanced searches, officers connect external equipment to the device to review, copy, or analyze its data. Id. at 5. Basic searches include all other searches, and therefore, do not involve the use of external equipment to review, copy, or analyze data. Id. at 4. Therefore, the search is significantly more restricted during basic searches. Id. See also Alasaad, 988 F.3d at 18 (reasoning that the amount of information available to agents during a basic electronics search is limited by the nature of the search). “The CBP Policy only allows searches of data resident on the device.” Id. at 18–19 (citing CBP Policies, supra note 5, at 4). “And a basic border search does not allow government officials to view deleted or encrypted files.” Id. at 19.

See CBP Policies, supra note 5, at 5 (describing the nature of advanced electronic device searches). “An advanced search is any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents.” Id. This external equipment used to review, copy, and analyze data grants access to significantly more information, in a shorter period, than does a basic search. Id. See also Protecting Client Data, supra note 1 (discussing concerns regarding searches of attorneys’ laptops containing privileged information, and the steps taken by the ABA to advocate for more stringent search requirements).

See Protecting Client Data, supra note 1 (advocating for stricter search procedures to protect confidential, privileged information on attorneys’ devices); Can Border Agents Search Your Devices, supra note 49 (discussing the ACLU’s objections to current border search policies). The ACLU argues that constitutional safeguards against unwarranted searches should apply in border zones as well due to the ubiquity of modern electronic devices and their growing capacity to store massive amounts of sensitive information. Id.
In the alternative, customs agents, at the very least, should be required to limit the scope of electronics searches to searches for digital contraband. Limiting the scope of these searches would still protect the privacy interests of travelers, albeit to a lesser degree than if the search itself was limited by a warrant requirement or by an individualized suspicion requirement. Customs officials need not waste their time searching aimlessly through documents unlikely to reveal digital contraband, such as attorney case materials, for example.

V. Conclusion

---

141 See Cano, 934 F.3d at 1018 (holding that border searches in Ninth circuit territory must be limited in scope to searches for contraband, and not searches for evidence of contraband) (emphasis added).

Our disagreement focuses precisely on the critical question that we previously identified: Does the proper scope of a border search include the power to search for evidence of contraband that is not present at the border? Or, put differently, can border agents conduct a warrantless search for evidence of past or future border-related crimes? We think that the answer must be “no.” The “[d]etection of . . . contraband is the strongest historic rationale for the border-search exception.”

142 See Cano, 934 F.3d at 1018 (justifying limiting the scope of the border search exception to searches for actual contraband because that is the “strongest historic rationale for the border-search exception.”). See also Protecting Client Data, supra note 1 (arguing that the law should require customs agents to have a greater standard of suspicion to search attorneys’ devices). Can Border Agents Search Your Devices, supra note 49 (discussing the ACLU’s objections to current border search policies). The ACLU argues that constitutional safeguards against unwarranted searches should apply in border zones as well. Id.

143 See Cano, 934 F.3d at 1018 (limiting the scope of the border search exception to searches for contraband, and not merely evidence of contraband). But see Alasaad, 988 F.3d at 20 (holding that searches for evidence of contraband fall under the border search exception because they are “vital to achieving the border search exception’s purposes of controlling ‘who and what may enter the country.’”).
International travelers attempting to enter the United States would benefit greatly from a uniform standard for searching their electronic devices in border zones. This standard would unify privacy protections for all international travelers, no matter which area of the country they seek to enter. That way, a traveler flying into Hawaii could expect the same privacy protections as one arriving in Florida.

In contemplating this standard, courts must consider the immense storage capacity of electronic devices, their ability to store private, intimate, and sensitive information, and their pervasiveness in today’s society. For these reasons, electronics searches in border zones should require a warrant, or alternatively, reasonable suspicion of criminal activity, because even basic electronics searches can uncover personal, intimate, and sensitive information. Furthermore, electronics searches should be limited in scope to searches for digital contraband.

Constitutional privacy protections of international travelers are at stake. These protections are especially vital for lawyers, who carry a professional duty to protect against the exposure of attorney-client privileged information. Courts maintain an important responsibility, not only to protect these indispensable privacy rights, but also to provide a clear and uniform standard for all travelers. International travelers, and especially lawyers, would benefit greatly from a stricter, uniform standard.