No. 25-4239

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
PLAINTIFF-APPELLEE,

v.

JOSE BELMONTE CARDOZO,
DEFENDANT-APPELLANT.

On Appeal from the United States District Court
For the Eastern District of Virginia

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, ELECTRONIC FRONTIER FOUNDATION, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, ACLU OF MARYLAND, ACLU OF NORTH CAROLINA, ACLU OF SOUTH CAROLINA, AND ACLU OF VIRGINIA IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

Michael W. Price
Litigation Director, Fourth Amendment Center
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
1660 L. St. NW, 12th Fl.
Washington, DC 20036
(202) 465-7615
mprice@nacdl.org

Nathan Freed Wessler
Esha Bhandari
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org
ebhandari@aclu.org

Elizabeth Franklin-Best
Vice Chair, Amicus Committee
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
Elizabeth Franklin-Best, P.C.
3710 Landmark Drive, Suite 113
Columbia, South Carolina 29204
(803) 445-1333
elizabeth@franklinbestlaw.com

Sophia Cope
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
sophia@eff.org

(Additional Counsel for Amici Curiae listed on following page)

Eden B. Heilman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF VIRGINIA
P.O. Box 26464
Richmond, VA 23261
(804) 523-2152
eheilman@acluva.org

David Rocah
AMERICAN CIVIL LIBERTIES UNION OF MARYLAND FOUNDATION
3600 Clipper Mill Road, Suite 200
Baltimore, MD 21211
(410) 889-8550, x. 111
rocah@aclu-md.org

Kristi L. Graunke
ACLU OF NORTH CAROLINA LEGAL FOUNDATION
P.O. Box 28004
Raleigh, NC 27611-8004
(919) 354-5066
kgraunke@acluofnc.org

Allen Chaney
AMERICAN CIVIL LIBERTIES UNION OF SOUTH CAROLINA FOUNDATION
P.O. Box 1668
Columbia, SC 29202
(864) 372-6681
achaney@aclusc.org

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amici curiae* American Civil Liberties Union, Electronic Frontier Foundation, National Association of Criminal Defense Lawyers, ACLU of Maryland, ACLU of North Carolina, ACLU of South Carolina, and ACLU of Virginia state that they do not have a parent corporation and that no publicly held corporation owns 10 percent or more of their stock.

Dated: October 28, 2025

/s/ Nathan Freed Wessler
Nathan Freed Wessler

Counsel for *Amici Curiae*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Regulations

Other Authorities

INTEREST OF *AMICI CURIAE*[1]

The American Civil Liberties Union (ACLU) is a nationwide, non-profit, non-partisan organization dedicated to defending the civil liberties and rights guaranteed by the Constitution. The ACLU of Maryland, ACLU of North Carolina, ACLU of South Carolina, and ACLU of Virginia are state affiliates of the national ACLU. The Electronic Frontier Foundation (EFF) is a non-profit public interest organization that works to ensure that constitutional rights are protected as technology advances. The National Association of Criminal Defense Lawyers (NACDL) is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct.

The ACLU and EFF were counsel in a civil case challenging the government's border device search policies and practices, *see Alasaad v. Mayorkas*, 988 F.3d 8 (1st Cir. 2021), *cert. denied, sub nom. Merchant v. Mayorkas*, 141 S. Ct. 2858 (2021), in which NACDL participated as *amicus*. ACLU, EFF, and NACDL have all participated as *amici* in multiple cases in federal circuit courts involving the application of the Fourth Amendment to border searches of electronic devices, including in this Circuit in *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018).

[1] Pursuant to Fed. R. App. P. 29(a)(4)(E), counsel for *amici curiae* certifies that no counsel for a party authored this brief in whole or in part, and no person other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission. Counsel for all parties consent to the filing of this brief.

SUMMARY OF ARGUMENT

This case presents an important question about the extent of Fourth Amendment privacy rights in the digital age. Most people carry electronic devices with them when they travel, including when they cross the nation's borders. Those devices contain an incredible volume and variety of personal information that can be revealed with a brief scroll through photos, messages, apps, or location history. Yet the government asserts the authority to manually search such devices at the border for any purpose, without a warrant, or even the minimum standard of individualized suspicion, effectively equating our capacious electronic devices with garden-variety physical luggage for Fourth Amendment purposes. As the Supreme Court made clear in *Riley v. California*, 573 U.S. 373 (2014), traditional exceptions to the Fourth Amendment's warrant requirement do not automatically apply to searches of cell phones and other electronic devices. In *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018), this Court protected privacy interests in such devices at the border by holding that individualized suspicion is required for forensic searches, and it should take this opportunity to hold that manual searches deserve, at minimum, the same Fourth Amendment protection. A lesser standard for manual searches would leave travelers vulnerable to the very privacy harms against which this Court sought to protect in *Kolsuz*.

Amici offer this brief to provide greater context about the growing practice of warrantless and suspicionless border searches of electronic devices nationwide, and to provide information about the magnitude of the privacy harm made possible by border officers' easy access to travelers' devices, regardless of whether a search is conducted manually or with additional forensic equipment.[2] *Amici* seek to demonstrate why this is an issue of widespread importance for civil liberties even outside of the context of criminal prosecutions. *Amici* also provide additional detail about how the Supreme Court's decision in *Riley* and the historical justifications for warrantless border searches affect the analysis of the constitutionality of forensic and manual device searches alike.

In *Kolsuz*, this Court held that forensic searches of electronic devices at the border must be supported by "some form of individualized suspicion" relating to an ongoing transnational crime. 890 F.3d at 143-46. And in *United States. v. Aigbekaen*, 943 F.3d 713 (4th Cir. 2019), the Court affirmed this minimum standard for forensic searches, confirming that the Government must have individualized suspicion of an offense that bears some nexus to the border-search exception's purposes. Importantly, while establishing that forensic searches require individualized

[2] In line with the terminology used in prior cases in this Circuit, this brief discusses "manual" and "forensic" searches. The government's relevant policies use the terms "basic" and "advanced," "[b]ut the import is the same." *Kolsuz*, 890 F.3d at 146 n.6.

suspicion, this Court did not decide whether reasonable suspicion is constitutionally adequate, holding open the possibility that the Fourth Amendment may require a warrant for these non-routine and invasive forensic searches. *See United States v. Nkongho*, 107 F.4th 373, 382 (4th Cir. 2024) ("[N]either *Kolsuz* nor *Aigbekaen* decided whether reasonable suspicion is enough to justify a forensic search or whether probable cause is required."); *Kolsuz*, 890 F.3d at 137. Further, this Court did not address whether a manual (but equally revealing) search of a device at the border may also constitute a non-routine search that requires at least individualized suspicion of an ongoing border-related crime. *Kolsuz*, 890 F.3d at 146 n.5 ("Because Kolsuz does not challenge the initial manual search of his phone at Dulles, we have no occasion here to consider whether *Riley* calls into question the permissibility of suspicionless manual searches of digital devices at the border.").

This case presents an opportunity for this Court to protect millions of innocent travelers who cross the U.S. border each year from arbitrary and extraordinarily invasive searches, by harmonizing its rule with *Riley* and holding that all electronic device searches require a warrant based on probable cause, irrespective of the method of search. Just as warrantless manual searches of cell phones were not justified by the purposes of the search-incident-to-arrest exception in *Riley*, here, similarly invasive manual and forensic searches of electronic devices are likewise

not justified by the rationales permitting warrantless border searches—namely, customs and immigration enforcement.

Even if this Court declines to require a warrant for all border device searches, it should hold that all device searches at the border, regardless of the government's method of search, require reasonable suspicion of contraband or an ongoing border-related offense, given the nearly identical privacy interests at stake. Indeed, a manual search of a device can be lengthy in duration, can uncover myriad pieces of sensitive personal information across many file types, and can utilize a device's native search tool to quickly search the entire contents of the device for keywords or images. The information on electronic devices is deeply sensitive and private, including personal correspondence, notes and journal entries, family photos, medical records, lists of associates and contacts, proprietary business information, attorney-client and other privileged communications, and more. This profoundly personal content is easily revealed through even a brief manual search, without the use of forensic technology.

Applying a uniform Fourth Amendment standard, in terms of the level and scope of suspicion required, for all device searches is critical because, as detailed below, manual device searches at the border are extraordinarily invasive and invite misuse as an end-run around the warrant requirement that normally applies to criminal investigations. The government should not get a loophole to conduct warrantless and suspicionless manual device searches for evidence of domestic

criminal activity simply because the target of an investigation has chosen to travel internationally. Such a rule aligns with the principles of *Riley* governing manual searches of devices and with the limited purposes of the border-search exception that this Court recognized in *Kolsuz* and *Aigbekaen*. In light of the increasing number of both manual and forensic border device searches, the failure to finally establish a robust Fourth Amendment standard for all device searches at the border exacerbates the "significant diminution of privacy" for travelers. *Riley*, 573 U.S. at 400.

ARGUMENT

I. A Uniform Standard is Needed Because Border Searches of Electronic Devices Are Increasing Rapidly and Affect Large Numbers of Travelers

Each year, hundreds of millions of people travel through border crossings, international airports, and other ports of entry into the United States.[3] Tens of thousands have their electronic devices searched, the vast majority of which are manual searches.[4] The government has justified its practice of searching electronic devices in part by noting that such searches are "rare,"[5] but border searches of

[3] *See* U.S. Customs & Border Prot., *Border Searches of Electronics at Ports of Entry, FY2024 Statistics* (2024), https://perma.cc/X7S7-8QME [hereinafter *CBP FY24 Statistics*].

[4] *See* U.S. Customs & Border Prot., *Border Search of Electronic Devices at Ports of Entry* (July 12, 2024), https://perma.cc/ZTY5-SPUE ("Of the 41,767 border searches of electronic devices encountered at port of entry, 37,778 (90%) were basic searches in which the devices were not connected to external equipment to review, copy and/or analyze its contents.").

[5] *Id.*

electronic devices have risen almost five-fold over the last decade. According to data from U.S. Customs and Border Protection (CBP), the agency conducted 47,047 device searches in fiscal year 2024,[6] compared to just 8,503 searches in fiscal year 2015.[7]

This Court should provide clarity to the government and the millions of international travelers who arrive and depart from the United States in the Fourth Circuit alone.[8] Moreover, as other cases have demonstrated, the government is conducting border device searches to advance pre-existing criminal investigations, including investigations of fraud and insurance crime that have nothing to do with the border at all. *See, e.g.*, *United States v. Smith*, 673 F. Supp. 3d 381 (S.D.N.Y. 2023) (insurance fraud); *United States v. Fox*, No. 23-CR-227, 2024 WL 3520767, at *11 (E.D.N.Y. July 24, 2024) (wire fraud).[9] This Court has already held that the "[g]overnment may not 'invoke[ ] the border exception [to the Fourth Amendment's warrant requirement] on behalf of its generalized interest in law enforcement and combatting crime." *Aigbekaen*, 943 F.3d at 721 (first alteration in original) (quoting

[6] *CBP FY24 Statistics*, *supra* note 3.

[7] Press Release, U.S. Customs & Border Prot., *CBP Releases Statistics on Electronic Device Searches* (Apr. 11, 2017), https://perma.cc/C7LQ-ZAN7.

[8] *See*, *e.g.*, Scott McCaffrey, *Dulles Airport's 2024 Passenger Total Set New All-time Record*, FFX Now (Mar. 3, 2025), https://perma.cc/S97P-VEU5.

[9] *Smith* is pending on appeal to the United States Court of Appeals for the Second Circuit.

Kolsuz, 890 F.3d at 143). However, absent a uniform, limiting rule from this Court on the merits of this Fourth Amendment question, the government will continue to use international travel by the targets of domestic criminal investigations as a convenient opportunity to sidestep the warrant requirements that would normally apply, simply by forgoing the use of forensic software and conducting manual, but similarly invasive, device searches—as it did in the instant case.

II. Travelers Have Extraordinary Privacy Interests in the Vast Quantities and Types of Personal Data Their Electronic Devices Contain

Riley recognized the unprecedented privacy interests people have in today's electronic devices. Even a relatively brief, manual search of a device can reveal the "sum of an individual's private life," and "bears little resemblance" to searches of bags or other containers, which are usually "limited by physical realities and tend[] as a general matter to constitute only a narrow intrusion on privacy." *Riley*, 573 U.S. at 386, 393–94. *Riley* explained that likening the search of ordinary physical items to the search of a cell phone "is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Id.* at 393. *Riley* held that electronic devices differ fundamentally—quantitatively and qualitatively—from physical containers. *Id*.

Quantitatively, with their "immense storage capacity," electronic devices contain "millions of pages of text, thousands of pictures, or hundreds of videos." *Riley*, 573 U.S. at 393–94. *See also United States v. Cotterman*, 709 F.3d 952, 964

(9th Cir. 2013) (en banc) ("The average 400-gigabyte laptop hard drive can store over 200 million pages—the equivalent of five floors of a typical academic library.").

Qualitatively, electronic devices "collect[] in one place many distinct types of information . . . that reveal much more in combination than any isolated record." *Riley*, 573 U.S. at 394. This information can include call logs, emails, voicemails, text messages, browsing history, calendar entries, contact lists, shopping lists, notes, photos and videos, other personal files, location information, and metadata. And a device does not just contain data stored locally, but also "data stored in the cloud that is temporarily cached on the device itself," and thus accessible even when a device is placed in "airplane mode" or otherwise disconnected from the internet, such as recent posts in social media apps. *United States v. Sultanov*, 742 F. Supp. 3d 258, 286 (E.D.N.Y. 2024). All of this information, in turn, can reveal—expressly or by inference—a detailed account of an individual's political affiliations, religious beliefs and practices, sexual and romantic lives, financial status, health conditions, and family and professional associations. *Riley*, 573 U.S. at 395–96. The privacy interests that travelers have in their electronic devices today are even greater than

those considered in *Riley* over a decade ago as the volume and types of data on devices continues to grow.[10]

III. Manual Searches of Electronic Devices are Highly Intrusive and Should Be Treated the Same as Forensic Searches for Fourth Amendment Purposes

Privacy interests in electronic devices are significant irrespective of the method of search; the government can access the same personally revealing information during both manual and forensic searches. Although forensic software can sometimes additionally uncover deleted, password-protected, or encrypted data, there is no "meaningful difference between the two classes of searches in terms of the privacy interests implicated." *Alasaad v. Nielsen*, 419 F. Supp. 3d 142, 165 (D. Mass. 2019).[11] Both methods of searching allow government agents to "peruse and search the contents of the device." *Id.* at 163. In a manual search, that can mean

[10] The new iPhone 17 Pro Max, for example, offers up to two terabytes of storage. Apple, *iPhone 17 Pro*, https://perma.cc/FUM5-BZ38. This is over 1500% more storage capacity than the 2014 model, which offered a maximum of 128 gigabytes of storage. Apple, *iPhone 6 – Technical Specifications*, https://perma.cc/7N7D-93DZ.

[11] Although the *Alasaad* district court's Fourth Amendment ruling was reversed on appeal, the First Circuit recognized that "[t]he material facts are not in dispute" and did not disturb those findings. *Alasaad v. Mayorkas*, 988 F.3d 8, 13 (1st Cir. 2021). The factual findings in that case were based on government testimony and documents that reflect their border search practices, and other facts that the government did not dispute. 419 F. Supp. 3d at 148 ("[T]he material facts concerning the searches of Plaintiffs' electronic devices and the policies pursuant to which CBP and ICE agents conduct border searches are undisputed.").

"using the native search functions on the device, including, if available, a keyword search." *Id.* "An agent conducting a basic search may use the device's own internal search tools to search for particular words or images. Accordingly, even a basic search allows for both a general perusal and a particularized search of a traveler's personal data, images, files and even sensitive information." *Id.* Moreover, these internal search tools are becoming more powerful and accurate. For example, the latest Apple operating system supports "natural language search in Photos," "live Translation in Messages," "Summaries in Mail and Messages," and other analytics tools, in addition to keyword searches of text in saved files, further increasing the invasiveness of a manual search.[12]

Manual searches can also be conducted over significant durations. In one case, for example, travelers' phones were subjected to manual searches spanning 37 minutes, 45 minutes, an hour, and an hour and a half, exposing "photos, emails and contacts," "journalistic work product," and myriad other material. *Alasaad*, 419 F. Supp. 3d at 164–65. A subsequent manual search of one of those travelers' phones exposed her privileged communications with her attorney in that very litigation. Decl. of Pl. Zainab Merchant ¶¶ 26–31, *Alasaad v. Nielsen*, No. 1:17-cv-11730 (D. Mass.) (ECF No. 91-7). Thus, "the distinction between manual and forensic searches

[12] Apple, *How to Get Apple Intelligence*, Apple Support (Oct. 9, 2025), https://perma.cc/3HMX-SMBW.

is too flimsy a hook on which to hang a categorical exemption to the Fourth Amendment's warrant requirement." *Sultanov*, 742 F. Supp. 3d at 290.

U.S. Department of Homeland Security policies distinguish between forensic and manual (or "advanced" and "basic") searches of electronic devices.[13] *Alasaad,* 419 F. Supp. 3d at 148. While that taxonomy may have utility in the government's internal management of its search activities, it makes no sense for Fourth Amendment purposes. *See Riley*, 573 U.S. at 398 (agency protocols may be a "good idea, but the Founders did not fight a revolution to gain the right to government agency protocols," and those protocols do not determine the Fourth Amendment rule). Indeed, the searches in *Riley* were manual, and the unanimous Court did not hesitate in requiring a warrant. *Id.* at 379–80. This Court has recognized as much: "*Riley* holds that the search incident to arrest exception … does not apply to *manual* searches of cell phones." *Kolsuz*, 890 F.3d at 145 (emphasis added). But because in *Kolsuz* the search in question was a forensic search, and the appellant disclaimed any challenge to the manual search that preceded it, the Court did not consider the constitutionality of warrantless and suspicionless manual searches at the border. *Id.* at 141. Yet, the reasoning in *Kolsuz*, and the specifics of the search at issue there, reveal the importance of a uniform rule. A manual search can reveal all that the

[13] *See* U.S. Customs & Border Prot., *CBP Directive 3340.049A: Border Search of Electronic Devices* (Jan. 4, 2018), https://perma.cc/HMQ2-AV2X.

Kolsuz court was concerned about, including "personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of [a person's] physical location down to precise GPS coordinates." *Id.* at 139. *Compare Riley*, 573 U.S. at 393–96 (cataloging types of information discoverable through manual search of a phone). *Kolsuz* recognized that the search in that case did not extend to "residual data of files that had been deleted by Kolsuz," which would only be accessible through forensic technology. 890 F.3d at 145 n.4. Yet, the Court expressly declined to distinguish "an extensive forensic search … from a *very* extensive forensic search," recognizing that such line drawing would not fairly account for the privacy interests at stake. *Id.*

This Court should now recognize that the privacy harms equally do not turn on whether a search is conducted with or without forensic software, given the user-friendly manual search functions, and the immense variety and volume of personal data, of modern devices. The government's use of forensic software may or may not reveal marginally more information in some circumstances, but ultimately, an extraordinary invasion of privacy occurs regardless of how a device is searched. This Court should therefore standardize the rule for both manual and forensic searches at the border, and decline to reinforce categories that are incompatible with *Riley*.

IV. The Fourth Amendment Requires a Warrant for Electronic Device Searches at the Border

This Court should hold that the border-search exception to the Fourth Amendment's warrant requirement does not apply to electronic devices like cell phones and laptops, and therefore a warrant based on probable cause is required for such searches. Since this Court's prior decisions holding that question open, several district courts have correctly applied the reasoning of *Riley* to conclude that a warrant is required for searches of electronic devices at the border. *See Smith*, 673 F. Supp. 3d at 396; *Sultanov*, 742 F. Supp. 3d 258; *Fox*, 2024 WL 3520767.

"The ultimate touchstone of the Fourth Amendment is reasonableness," which generally means that a warrant based on probable cause is required for a government search. *Riley*, 573 U.S. at 381–82 (cleaned up). However, warrantless, suspicionless searches may be reasonable when justified by a "primary purpose" that is "beyond the normal need for law enforcement" or "beyond the general interest in crime control." *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653, 665 (1995) (cleaned up) (upholding drug tests to protect the health and safety of minor student athletes, not to find evidence to prosecute drug crimes); *City of Indianapolis v. Edmond*, 531 U.S. 32, 37, 42, 48 (2000) (striking down vehicle checkpoint to uncover illegal narcotics because its primary purpose was to "uncover evidence of ordinary criminal wrongdoing").

In determining whether to apply an existing warrant exception to a "particular category of effects" such as cell phones and other electronic devices, individual privacy interests must be balanced against legitimate governmental interests. *Riley*, 573 U.S. at 385–86. Crucially, governmental interests are weak where warrantless searches are "untether[ed]" from the non-criminal, non-law enforcement purposes justifying the exception at issue. *Id.* at 386. Thus, *Riley* held that there is a weak nexus between warrantless searches of arrestees' cell phones and the purposes of the search-incident-to-arrest exception—protecting officer safety and preventing the destruction of evidence—because such warrantless searches do not sufficiently advance those goals. *Id.* at 387–91. *See also Florida v. Royer*, 460 U.S. 491, 500 (1983) (warrantless searches "must be limited in scope to that which is justified by the particular purposes served by the exception"). That required balancing leads to an analogous conclusion here, whether a search is conducted with or without forensic technology.

Warrantless searches of electronic devices do not sufficiently advance the goals of the border-search exception, which are limited to preventing the entry of inadmissible goods and persons. *See Carroll v. United States*, 267 U.S. 132, 154 (1925) (an international traveler may be required to "identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in"); *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985) (emphasizing the

government's interest in collecting duties and preventing "the introduction of contraband into this country."); *United States v. 12 200-Foot Reels of Super 8mm. Film*, 413 U.S. 123, 125 (1973) (government interest is in "prevent[ing] smuggling and … prohibited articles from entry"); *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971) (inspecting luggage "is an old practice and is intimately associated with excluding illegal articles from the country"). Thus, "[d]etection of … contraband is the strongest historic rationale for the border-search exception." *United States v. Molina-Isidoro*, 884 F.3d 287, 295 (5th Cir. 2018) (Costa, J., specially concurring); *accord United States v. Cano*, 934 F.3d 1002, 1018 (9th Cir. 2019) (citing Judge Costa).

In light of these traditional justifications for the border-search exception, the government's "interest in searching the digital data 'contained' on a particular physical device located at the border is relatively weak." *Smith*, 673 F. Supp. 3d at 395 (citation omitted). As with the search-incident-to-arrest exception, the border-search exception may "strike[] the appropriate balance in the context of physical objects" such as luggage and vehicles, but its underlying rationales lack "much force with respect to digital content on cell phones" or other electronic devices. *See Riley*, 573 U.S. at 386. Further, *Riley* required a warrant to search the cell phones of arrestees despite their "diminished privacy interests." *Id.* at 392. Likewise, although travelers also have a diminished expectation of privacy at the border, *Montoya de*

Hernandez, 473 U.S. at 539, "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse," *Riley*, 573 U.S. at 393. Moreover, the overwhelming majority of international travelers are not suspected of any crime, unlike arrestees. Ultimately, because travelers' extraordinary privacy interests outweigh any legitimate governmental interests, border searches of electronic devices require a warrant based on probable cause. *See Smith*, 673 F. Supp. 3d at 396.

Requiring a warrant is consistent not only with *Riley*, but with the Supreme Court's border-search cases that have contemplated that some warrantless border searches may be unreasonable "because of the particularly offensive manner in which [they are] carried out." *United States v. Flores-Montano*, 541 U.S. 149, 154 n.2 (2004) (quoting *United States v. Ramsey*, 431 U.S. 606, 618 n.13 (1977)). The Court has never suggested that reasonable suspicion is a ceiling, rather than a floor, for highly invasive border searches. *See Montoya de Hernandez,* 473 U.S. at 541 n.4 (declining to decide "what level of suspicion" is required for highly intrusive searches); *Flores-Montano*, 541 U.S. at 152. In *Ramsey*, the Court left open the possibility that where border searches burden First Amendment rights, the "full panoply" of Fourth Amendment protections—*i.e.*, a warrant—might apply. 431 U.S. at 623–24, 624 n.18.

It is already the law of this Circuit that warrants are required to search electronic devices seized at the border in some circumstances—namely, when the government seeks evidence unrelated to a border-related offense. *Aigbekaen*, 943 F.3d at 721. This Court, should now hold that a warrant is required for electronic device searches at the border in *all circumstances*—given travelers' extraordinary privacy interests in their digital data, and given that the government's interests in conducting warrantless device searches are untethered from the border-search exception's traditional justifications of preventing unwanted persons or things from entering the country. Further, as explained above, there is no basis for a different Fourth Amendment rule for manual searches, given how highly invasive they are. *See supra* Part III.

A warrant requirement would not impede the government's border enforcement activities. Border officers could still search without a warrant the "physical aspects" of an electronic device, such as a laptop battery compartment to ensure that it does not contain drugs or explosives. *See Riley*, 573 U.S. at 387. Where border officers have probable cause that the data on a device contains evidence of wrongdoing, they can secure a search warrant. The process of getting a warrant is not unduly burdensome. As *Riley* explained, "[r]ecent technological advances … have … made the process of obtaining a warrant itself more efficient." *Id.* at 401. The government has experience in obtaining warrants for searches of electronic

devices and in other contexts at the border.[14] Additionally, getting a warrant would not impede the efficient processing of travelers. If border officers have probable cause to search a device, they may retain it and let the traveler continue on their way, then get a search warrant. Or, where there is truly no time to go to a judge, the exigent circumstances exception may apply on a case-by-case basis. *See Riley*, 573 U.S. at 388, 391, 402.

V. Absent a Warrant, the Fourth Amendment Requires At Least Reasonable Suspicion of a Border-Related Crime for All Electronic Device Searches at the Border

If this Court declines to hold that all border searches of electronic devices require a warrant, it should extend *Kolsuz* and rule that all device searches—whether manual or forensic—must be treated as non-routine searches, supported by reasonable suspicion that the device contains either contraband or evidence of transnational crime *and* be limited in scope to searching for that material. Not only does this rule remain faithful to *Riley* and related Supreme Court cases, it is consistent with this Court's jurisprudence.

[14] *See* U.S. Dep't of Homeland Sec., DHS/CBP/PIA-053, *Privacy Impact Assessment for the U.S. Border Patrol Digital Forensics Programs* 1–2 (Apr. 6, 2018), https://perma.cc/HUY4-KWHD; U.S. Customs & Border Prot., Off. of Field Operations, CIS HB 3300-04C, *Personal Search Handbook* 37, 40 (Apr. 2021), https://perma.cc/8GR9-T65S; 19 C.F.R. § 145.3(b) (warrant required to open mail containing only correspondence).

First, manual device searches at the border are highly invasive and therefore properly categorized as non-routine searches requiring at least reasonable suspicion. In distinguishing between routine and nonroutine border searches, courts look to how deeply the search intrudes into a person's privacy. *Kolsuz,* 890 F.3d at 144. Under that approach, "border searches of luggage, outer clothing, and personal effects consistently are treated as routine, while searches that are most invasive of privacy—strip searches, alimentary-canal searches, x-rays, and the like—are deemed nonroutine and permitted only with reasonable suspicion." *Id*. In designating forensic device searches as non-routine, this Court noted that "while an international traveler can mitigate the intrusion occasioned by a routine luggage search by leaving behind her diaries, photographs, and other especially personal effects . . . it is neither 'realistic nor reasonable to expect the average traveler to leave his digital devices at home when traveling.' *Id.* at 145 (quoting *United States v. Saboonchi*, 990 F. Supp. 2d 536, 556 (D. Md. 2014)). This Court should now decline to make a distinction in the level of suspicion required between manual and forensic searches, given that manual searches can and do reveal the same highly sensitive private information as forensic searches and *Riley* involved a manual cell phone search. It is not the use of forensic software that exceeds the bounds of a routine border search; rather it is the core act of intruding into private digital content stored on electronic devices. Because both manual and forensic searches are extraordinarily invasive, all

electronic device searches should be uniformly treated as non-routine border searches requiring at least reasonable suspicion. *See supra* Part III.

Second, limiting the scope of reasonable suspicion to whether the device contains digital contraband or evidence of a border-related crime and limiting the scope of the actual search to such content are also necessary. If a warrantless search is to be permissible, in the absence of the privacy protections of the warrant process—the attendant findings of probable cause and particularity by a neutral and detached magistrate—the search must hew closely to the warrant exception's purported purposes. *See, e.g.*, *Arizona v. Gant*, 556 U.S. 332, 343 (2009). The Supreme Court has made clear that although some warrant exceptions, like border searches, might result in "arrests and criminal prosecutions," that does not mean that the exceptions were "designed primarily to serve the general interest in crime control." *Edmond*, 531 U.S. at 42. This Court has already ruled that a warrant is required when a *forensic* device search is in furtherance of a domestic criminal investigation and is thus "entirely unmoored" from "the recognized historic rationales justifying the border search exception." *Aigbekaen*, 943 F.3d at 721. This Court should now establish that this rationale must similarly apply to non-forensic searches as well, given the virtually identical privacy interests. Granting the government authority to manually search devices without suspicion and for evidence for any purpose would open the door to invasive searches that would normally

require a warrant if the target never happened to travel internationally. If this Court declines to hold the government to a uniform standard for manual and forensic searches, then it will be permitting an enormous end-run around *Kolsuz* and *Aigbakaen* to conduct extraordinarily invasive searches for any purpose, simply by refraining from using forensic software.

CONCLUSION

Amici respectfully urge this Court to hold that the Fourth Amendment requires border officers to obtain a warrant before conducting any electronic device search at the border, or at least decline to create a separate standard for manual searches. Given the indistinguishable privacy interests implicated by forensic and manual searches of modern devices, this Court should at minimum require reasonable suspicion that the device contains either contraband or evidence of transnational crime, regardless of the method of search.

October 28, 2025

Respectfully submitted,

/s/ Nathan Freed Wessler

Sophia Cope
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
sophia@eff.org

Nathan Freed Wessler
Esha Bhandari
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org
ebhandari@aclu.org[15]

[15] Counsel thank law graduate Byul Yoon, who contributed to drafting of this brief.

Michael W. Price
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
1660 L. St. NW, 12th Fl.
Washington, DC 20036
mprice@nacdl.org
(202) 465-7615

Eden B. Heilman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF VIRGINIA
P.O. Box 26464
Richmond, VA 23261
(804) 523-2152
eheilman@acluva.org

Kristi L. Graunke
ACLU OF NORTH CAROLINA LEGAL FOUNDATION
P.O. Box 28004
Raleigh, NC 27611-8004
(919) 354-5066
kgraunke@acluofnc.org

Elizabeth Franklin-Best
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
Elizabeth Franklin-Best, P.C.
3710 Landmark Drive, Suite 113
Columbia, South Carolina 29204
elizabeth@franklinbestlaw.com
(803) 445-1333

David Rocah
AMERICAN CIVIL LIBERTIES UNION OF MARYLAND FOUNDATION
3600 Clipper Mill Road, Suite 200
Baltimore, MD 21211
(410) 889-8550, x. 111
rocah@aclu-md.org

Allen Chaney
AMERICAN CIVIL LIBERTIES UNION OF SOUTH CAROLINA FOUNDATION
P.O. Box 1668
Columbia, SC 29202
(864) 372-6681
achaney@aclusc.org

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7) and Fed. R. App. P. 29(a)(5) because it contains 5,147 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

This brief also complies with the typeface and type-style requirements of Fed. R. App. P. 32(a)(5)–(6) because it was prepared using Microsoft Word in Times New Roman 14-point font, a proportionally spaced typeface.

Dated October 28, 2025

/s/ Nathan Freed Wessler
Nathan Freed Wessler

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on October 28, 2025, I electronically filed the foregoing Brief of *Amici Curiae* with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system. Participants in the case are registered CM/ECF users, and service will be accomplished by the appellate CM/ECF system.

/s/ Nathan Freed Wessler
Nathan Freed Wessler

Counsel for Amici Curiae