No. 24-1680

IN THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

UNITED STATES OF AMERICA,

APPELLEE,

v.

SEQUAN JACKSON, AKA SEALED DEFENDANT 2, ANTHONY MCGEE, AKA SEALED DEFENDANT 3, KAHEEN SMALL, AKA SEALED DEFENDANT 4, DAMON DORE, AKA SEALED DEFENDANT 5, HASIM SMITH, AKA SEALED DEFENDANT 6, RAHMIEK LACEWELL, AKA SEALED DEFENDANT 7, MANUEL PEREIRA, AKA SEALED DEFENDANT 8, OCTAVIO PERALTA, AKA SEALED DEFENDANT 9, CARL WALSH,

DEFENDANTS,

JATIEK SMITH, AKA SEALED DEFENDANT 1

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
For the Southern District of New York

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, ELECTRONIC FRONTIER FOUNDATION, AND NEW YORK CIVIL LIBERTIES UNION IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

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

NEW YORK CIVIL LIBERTIES UNION FOUNDATION
Molly Biklen
125 Broad Street, 19th Floor
New York, NY 10004
(212) 607-3300
mbiklen@nyclu.org

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

Counsel for Amici Curiae

November 22, 2024

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amici curiae* American Civil Liberties Union, Electronic Frontier Foundation, and New York Civil Liberties Union state that they do not have a parent corporation and that no publicly held corporation owns 10 percent or more of their stock.

Dated: November 22, 2024

/s/ Esha Bhandari
Esha Bhandari

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

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 New York Civil Liberties Union is a state affiliate 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 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), and have argued as *amici* in multiple cases in federal circuit courts involving the application of the Fourth Amendment to border device searches.

[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. Yet the government asserts the authority to search such devices without any individualized suspicion, much less a warrant, whenever an individual seeks to enter or exit the country, 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), however, traditional exceptions to the Fourth Amendment's warrant requirement do not automatically apply to searches of cell phones and other electronic devices. Just as warrantless searches of cell phones were not justified by the purposes of the search-incident-to-arrest exception in *Riley*, here, unfettered searches of electronic devices are likewise not justified by the rationales permitting warrantless border searches—namely, customs and immigration enforcement. The district court properly applied *Riley* in analyzing the constitutionality of warrantless border device searches.

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. This Court's decision will impact millions of innocent travelers who cross the U.S. border each year carrying laptops, smartphones, and other electronic devices. *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 device searches.

This Court should hold, as the district court correctly did, that border searches of electronic devices may not be conducted without a warrant based on probable cause given the unprecedented privacy interests at stake. The information on electronic devices can be 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. In light of the increasing number of border device searches, the failure to articulate the appropriate standard may result in a "significant diminution of privacy" for travelers. *Id.* at 400.

But even if this Court declines to require a warrant for border device searches, it should adopt the Ninth Circuit's rule and require that the government have reasonable suspicion that a device contains digital contraband, and that any search be limited to looking for digital contraband. *See United States v. Cano*, 934 F.3d

1002 (9th Cir. 2019). This Court should extend the Ninth Circuit's rule for forensic searches to all device searches at the border, whether manual or forensic, given the nearly identical privacy interests.

Limiting device searches to digital contraband is vital because warrantless device searches at the border are being routinely misused as an end-run around the warrant requirement that normally applies to criminal investigations. This case is a prime example, where border officers used a warrantless device search to advance a domestic insurance fraud investigation. Simply because the target of an investigation has chosen to travel internationally should not give the government a loophole to search for evidence of criminal activity without a warrant. Even if the government is permitted to conduct a warrantless search at the border, it should be prevented from engaging in a wide-ranging investigative search for criminal evidence and should instead be limited to a search tethered to its interests *at the border*—namely, interdicting digital contraband. Such a rule aligns with the limited purposes of the border-search exception.

ARGUMENT

I. This Court's Guidance 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.[2] Tens of thousands have their electronic devices searched. The government has justified its practice of searching electronic devices in part by noting that such searches are "rare,"[3] but border searches of electronic devices have risen almost five-fold in eight years. According to data from U.S. Customs and Border Protection (CBP), the agency conducted 41,767 device searches in fiscal year 2023,[4] compared to just 8,503 searches in fiscal year 2015.[5]

This Court has never addressed the Fourth Amendment's application to searches of electronic devices at the border, much less since the Supreme Court made clear in *Riley* that any exception to the warrant requirement must be considered anew with respect to searches of electronic devices. Although *amici* agree with Defendant-

---

[2] *See* U.S. Customs and Border Protection, *Border Searches of Electronics at Ports of Entry, FY2023 Statistics* (July 5, 2024) [hereinafter *CBP FY23 Statistics*], https://perma.cc/2SHP-4LYF.
[3] U.S. Customs and Border Protection, *Border Search of Electronic Devices at Ports of Entry* (July 12, 2024), https://perma.cc/ZTY5-SPUE.
[4] *CBP FY23 Statistics*, *supra* n.2.
[5] U.S. Customs and Border Protection, *CBP Releases Statistics on Electronic Device Searches* (Apr. 11, 2017), https://perma.cc/C7LQ-ZAN7.

Appellant that the good-faith exception to the exclusionary rule does not properly apply in this case, even if this Court disagrees, it should provide clarity to the government and the millions of international travelers who arrive and depart from the United States in this circuit alone.[6] Moreover, as this case and others in this circuit 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* SPA 5-8, ECF No. 19.1; *United States v. Fox*, No. 23-CR-227, 2024 WL 3520767 at *11 (E.D.N.Y. July 24, 2024). Absent a limiting rule on the merits of the Fourth Amendment question from this Court, the government will continue to use international travel by the targets of investigations as a convenient opportunity to sidestep the warrant requirements that would normally apply to such criminal investigations.

II. The Fourth Amendment Balancing Test in *Riley* Governs Whether the Border-Search Exception to the Warrant Requirement Applies to Electronic Devices

"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

[6] *See* Port Auth. of N.Y. and N.J., *2023 Airport Traffic Report* 47 (Apr. 2024), https://perma.cc/UL64-LQCN.

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.

III. 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. A device search 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 claiming that searches of physical items are the same as those of digital data "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*. This Court has also recognized that "the search and seizure of personal electronic devices … implicates different privacy and possessory concerns than the search and seizure of a person's ordinary personal effects." *United States v. Smith*, 967 F.3d 198, 208 (2d Cir. 2020). *See also United States v. Ganias*, 824 F.3d 199, 217 (2d Cir. 2016).

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, such as recent posts in social media apps. *United States v. Sultanov*, No. 22-CR-149, 2024 WL 3520443 at *18 (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.

Moreover, 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.[7]

Importantly, privacy interests in electronic devices are significant irrespective of the method of search. U.S. Department of Homeland Security policies distinguish

[7] The new iPhone 16 Pro, for example, offers one terabyte of storage. Apple, *iPhone 16 Pro Tech Specs*, https://perma.cc/C5FL-4XPE.

between forensic and manual (or "advanced" and "basic") searches of electronic devices, *Alasaad v. Nielsen*, 419 F. Supp. 3d 142, 148 (D. Mass. 2019), and some courts have required individualized suspicion for forensic but not manual searches at the border. *See, e.g.*, *Cotterman*, 709 F.3d at 966-67. But that distinction makes no sense for Fourth Amendment purposes. The searches in *Riley* were manual, and the unanimous Court did not hesitate in requiring a warrant. 573 U.S. at 379-80. That is because the government can access the same personally revealing information during manual and forensic searches, notwithstanding that forensic searches can sometimes additionally uncover deleted, password-protected, or encrypted data. *Alasaad*, 419 F. Supp. 3d at 165.[8] Thus, "the distinction between manual and forensic searches is too flimsy a hook on which to hang a categorical exemption to the Fourth Amendment's warrant requirement." *Sultanov*, 2024 WL 3520443 at *22. Further, *Riley* required a warrant to search the cell phones of arrestees despite their "diminished privacy interests." *Riley*, 573 U.S. at 392. Likewise, although travelers also have a diminished expectation of privacy at the border, *United States v. Montoya de Hernandez,* 473 U.S. 531, 539 (1985), "[m]odern cell phones, as a category,

[8] Although the *Alasaad* district court's Fourth Amendment ruling was reversed on appeal, the First Circuit recognized that "the 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.

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.

IV. Warrantless and Suspicionless Electronic Device Searches Are Untethered from the Border-Search Exception's Purposes

Electronic device searches do not fall within the traditional border-search exception to the Fourth Amendment's warrant requirement, because they constitute an extraordinary privacy invasion and are not tethered to the exception's justifications. The Supreme Court has emphasized that warrantless border searches are justified only by the limited purposes of 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").

For over a century, however, the Court has repeatedly focused on customs enforcement, suggesting that it is the primary justification for the border-search exception. Specifically, the Court has emphasized the government's interest in collecting duties and preventing "the introduction of contraband into this country." *Montoya de Hernandez*, 473 U.S. at 537. Customs enforcement includes "protecting this Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics, or explosives." *Id.* at 544. *See also 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 Cano*, 934 F.3d at 1018 (citing Judge Costa).

A. Warrantless Border Device Searches Are Not Sufficiently Tethered to Interdicting Physical or Digital Contraband

Physical Contraband. The historic customs rationale for the border-search exception is to prevent *physical items* from entering the country at the moment the traveler crosses the border, either because the items were not declared for duties or would be harmful if brought into the country. This is constitutionally effectuated when border officers search travelers' luggage, vehicles, and, if necessary, their persons without a warrant. *See*, *e.g.*, *United States v. Flores-Montano*, 541 U.S. 149, 151 (2004) (inspecting vehicle gas tank for drugs); *Montoya de Hernandez*, 473 U.S. at 544 (inspecting traveler for drugs).

However, warrantless searches of electronic devices are untethered from this primary purpose. Just as *Riley* stated that "data on the phone can endanger no one" in relation to the search-incident-to-arrest exception's purpose of protecting officer safety, 573 U.S. at 387, physical contraband cannot be hidden in digital data. *See*

Molina-Isidoro, 884 F.3d at 295 (Costa, J., specially concurring) (physical contraband "cannot be stored within the data of a cell phone" and "this detection-of-contraband justification would not seem to apply to an electronic search of a cellphone or computer"); *United States v. Vergara*, 884 F.3d 1309, 1317 (11th Cir. 2018) (J. Pryor, J., dissenting) ("[T]he rationales underlying the border search exception lose force when applied to" device searches because they "do not contain the physical contraband that border searches traditionally have prevented from crossing the border.").

Digital Contraband. The government's interest in conducting warrantless device searches to interdict digital contraband is weak because the *Riley* factors are not satisfied.

First, in contrast to physical contraband like drugs, digital contraband is not a "prevalent" problem at the border. *See Riley*, 573 U.S. at 389. As the district court concluded in *Alasaad*, the government had proffered a "dearth of information of the prevalence of digital contraband entering the U.S. at the border." 419 F. Supp. 3d at 158. Digital content that is itself unlawful is limited. As the Ninth Circuit stated, "the detection-of-contraband justification would rarely seem to apply to an electronic search of a cell phone outside the context of child pornography." *Cano*, 934 F.3d at 1021 n.13. And according to the federal government, child pornography is primarily

accessed in the U.S. via the internet.[9] For fiscal year 2019, child pornography offenders in the U.S. almost entirely used the internet to either receive or distribute child pornography.[10]

Second, the government has not shown "that the ability to conduct a warrantless search would make much of a difference" in preventing the importation of digital contraband into the country. *See Riley*, 573 U.S. at 390. With *physical* contraband like drugs, warrantless searches of luggage or vehicles do make a difference because any drugs the government interdicts at a port of entry cannot be imported. But unlike physical contraband, digital contraband can exist in multiple copies, and is easily transported across borders via the internet. *See Alasaad*, 419 F. Supp. 3d at 158, 162. When the government interdicts digital contraband, it is likely that *identical* data has already entered the U.S. and been distributed widely via the internet.

District courts in this circuit have rightly recognized this important fact. In explaining why cell phone searches at the border should generally require a warrant, the district court here stated:

---

[9] U.S. Dep't of Just., *Subject Matter Expert Working Group Report: Child Sexual Abuse Material* 3-4 (2023), https://perma.cc/2279-5ZSV. ("[B]ecause [Child Sexual Abuse Material] is available through so many internet locations, offenders can access and demand CSAM repeatedly, any time they desire, without the need to store the files on their own devices.").

[10] U.S. Sent'g. Comm'n., *Federal Sentencing of Child Pornography: Non-Production Offenses* 32-34 (June 29, 2021), https://perma.cc/24F4-424E.

> When the Government interdicts contraband … it successfully stops a person or thing outside the country from unlawfully coming into it. But data stored on a cell phone … can and very likely does exist not just on the phone device itself … Stopping the cell phone from entering the country would not … mean stopping the data contained on it from entering the country.

SPA 20, ECF No. 19.1. *See also Sultanov*, 2024 WL 3520443 at *17-18 ("Searching and seizing the data on a person's phone does not prevent that data, which the cell phone holder all but certainly obtained and/or stores outside the device, from entering and circulating within the country."). *Accord Vergara*, 884 F.3d at 1317 (J. Pryor, J., dissenting) ("electronic contraband is borderless").

Although some travelers' devices might contain one of the few types of digital contraband, that does not justify a *categorical* rule permitting warrantless border searches of all devices.

B. The Government Has No Cognizable Interest in Conducting Warrantless Border Device Searches to Gather Evidence of Border Crimes or for General Law Enforcement

Consistent with Supreme Court jurisprudence related to warrant exceptions generally, *see supra* Part II, searching for *evidence* of border crimes—including evidence of contraband smuggling—or evidence for general law enforcement is outside the scope of the narrow primary purpose of the border-search exception, which is to find dutiable or prohibited goods themselves.

As the Supreme Court explained over a century ago in *Boyd v. United States*, customs enforcement focuses on the search and seizure of "goods liable to duties

and concealed to avoid the payment thereof," and *not* the "search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him." 116 U.S. 616, 623 (1886).[11] As Judge Costa of the Fifth Circuit has explained, following *Boyd*, "no … tradition exists for unlimited authority to search and seize items that might help to prove border crimes but are not themselves instrumentalities of the crime." *Molina-Isidoro*, 884 F.3d at 297 (Costa, J., specially concurring). That is because *Boyd*'s "emphatic distinction between the sovereign's historic interest in seizing imported contraband and its lesser interest in seizing records revealing unlawful importation" has special relevance in the context of "electronic data that cannot conceal contraband and that, to a much greater degree than the papers in *Boyd*, contains information that is like an extension of the individual's mind." *Id*.

Meanwhile, gathering evidence for general law enforcement is completely untethered from the border-search exception's permissible purposes. Yet the government routinely engages in this practice. In *Alasaad*, the district court found that the government conducts warrantless device searches to seek evidence of

[11] While *Warden v. Hayden*, 387 U.S. 294, 306-07, 309-10 (1967), overruled *Boyd* in part, it only collapsed the distinction between searches for contraband and searches for evidence for warrant-based searches given their privacy safeguards. *See also Molina-Isidoro*, 884 F.3d at 296 n.7 (Costa, J., specially concurring) ("Although *Hayden* is viewed as a broad rejection of the 'mere evidence'/instrumentality distinction … there are reasons to believe the distinction still matters when it comes to border searches.").

"illegal activities" separate and apart from searches for the admissibility of goods or persons. 419 F.Supp.3d at 157. *Alasaad* was the only case after *Riley* that featured civil discovery allowing examination of the government's border device search practices outside the context of any particular criminal prosecution, and in which the border agencies testified about their purposes in conducting border device searches. That testimony revealed an astonishing breadth of claimed authority by CBP and U.S. Immigration and Customs Enforcement, including to gather evidence about violations of a wide range of laws such as financial, tax, environmental, consumer protection, and other laws. The agencies also claimed the authority to conduct warrantless searches of electronic devices for intelligence gathering, and even to search the devices of travelers who are not themselves suspected of any wrongdoing to gather evidence about *other people*, such as searching a journalist's or scholar's device when they have foreign sources of interest to the government; a U.S. citizen's device for information about a suspected undocumented immigrant; and a traveler's device for evidence of their business partner's or family member's suspected wrongdoing. Such searches are often at the behest of other federal agencies, including the IRS, the FBI, and local police,[12] as was the case here. SPA 6, ECF No. 19.1 (FBI requested device search).

[12] *See* Pls.' Statement of Undisputed Material Facts ¶¶ 84-90, ECF No. 90-2, *Alasaad v. Nielsen*, 419 F. Supp. 3d 142 (D. Mass. 2019), available at https://perma.cc/T6V5-NA4J.

Yet the government's interest in finding evidence for general law enforcement is no greater at the border than anywhere else. The government thus unconstitutionally "use[s] the border-search exception to shirk the warrant requirement that otherwise applies to cellphones." *Fox*, 2024 WL 3520767 at *17 (requiring a warrant and granting suppression where the cell phone search at the border was seeking evidence of a domestic financial crime). As the Fourth Circuit emphasized, "the Government may not 'invoke[] the border exception on behalf of its generalized interest in law enforcement and combatting crime.'" *United States v. Aigbekaen*, 943 F.3d 713, 721 (4th Cir. 2019). *See also Molina-Isidoro*, 884 F.3d at 296 (Costa, J., specially concurring) (questioning whether an "evidence-gathering justification is so much stronger at the border that it supports warrantless and suspicionless searches of the phones of the millions crossing it"); *Vergara*, 884 F.3d at 1317 (J. Pryor, J., dissenting) (a "general law enforcement justification" does not support warrantless cell phone searches at the border because this justification is "quite far removed from the purpose originally underlying the border search exception"). Accordingly, the warrantless access to Defendant-Appellant's cell phone data here was not justified by border officers' belief that he was engaged in domestic insurance fraud related to the emergency mitigation services industry. SPA 5-6, ECF No. 19.1.

To be sure, this Court held in *United States v. Levy* that border officers could copy a paper notebook found in luggage without a warrant (but with reasonable suspicion) in furtherance of a non-border-related criminal investigation. 803 F.3d 120, 121 (2d Cir. 2015). But the *Riley* Court made clear that the distinction between physical records and digital ones requires an entirely separate privacy analysis and balancing of interests under the Fourth Amendment, writing that

> the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years. And to make matters worse, such an analogue test would allow law enforcement to search a range of items contained on a phone, even though people would be unlikely to carry such a variety of information in physical form.

Riley, 573 U.S. at 400. While the physical limitations of what travelers can carry necessarily limits the privacy harms of warrantless searches of their physical items, border device searches demand a different "categorical rule." *See id.* at 394, 398.

Indeed, *Riley* acknowledged that the "pre-digital" rule for searches-incident-to-arrest would have allowed officers to conduct some searches that were not strictly tethered to the justifications underlying the exception. *Riley* discussed *United States v. Robinson*, 414 U.S. 218 (1973), in which a search of the inside of a cigarette pack, revealing heroin, was deemed permissible "even though there was no concern about the loss of evidence, and the arresting officer had no specific concern that Robinson might be armed." *Riley*, 573 U.S. at 384. *Riley* noted that warrant exceptions do not

require "case-by-case adjudication" for the justification behind each individual search, and therefore concluded that simply because "police are entitled to open a pocket diary to copy the owner's address" upon arrest—conduct similar to that in *Levy*—does *not* mean they should be able to obtain the same information from a cell phone search. *Id*. at 384, 400.

C. Warrantless Border Device Searches Are Not Sufficiently Tethered to Preventing the Entry of Inadmissible Persons

Border officers determine a traveler's immigration status and authority to enter the U.S. by inspecting official documents such as passports and visas and questioning travelers.[13] As the district court in *Alasaad* recognized, the government does not need unbounded access to travelers' electronic devices in order to prevent the entry of inadmissible persons when those travelers are U.S. citizens and lawful permanent residents who are automatically admissible. *Alasaad*, 419 F. Supp. 3d at 158. As for those who are not U.S. persons, "where CBP posits that an electronic device might contain contradictory information about his/her intentions to work in the U.S. contrary to the limitations of a visa," the *Alasaad* court found after discovery that "there is no indication as to the frequency of same or the necessity of unfettered

[13] *See* U.S. Customs and Border Protection, *Immigration Inspection Program* (March 6, 2024), https://perma.cc/WZL8-YP64 ("U.S. citizens are automatically admitted upon verification of citizenship; aliens are questioned and their documents are examined to determine admissibility….").

access to the trove of personal information on electronic devices for this purpose." *Id.* at 167.

Ultimately, as the district court here recognized, even if

> data may contain information relevant … to whether a person should be allowed entry, … the Government has little heightened interest in blocking entry of the information itself, which is the historical basis for the border search exception. The Government's more general investigative interest in data *about* the person or thing entering the country is entirely incidental to the fact of the cell phone being carried over the border, and could just as easily be relied upon to support searches of the person's home, records, or past mail far away from the border.

SPA 27, ECF No. 19.1.

In sum, the government's permissible interests in conducting warrantless and suspicionless border device searches are: (1) weak as to interdicting physical and digital contraband; (2) nonexistent as to gathering evidence for any purpose; (3) nonexistent as to determining the admissibility of U.S. persons; and (4) weak as to preventing the entry of inadmissible foreign nationals. Moreover, even if the government's interests in conducting warrantless border device searches were not insubstantial, they do "not justify dispensing with the warrant requirement across the board." *Riley*, 573 U.S. at 388. Travelers' extraordinary privacy interests in their digital data outweigh any legitimate governmental interests.

V. 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. Applying the reasoning of *Riley*, the district court here and several others in this circuit have correctly concluded that a warrant is required for border device searches. *See* SPA 19, 29-30, ECF No. 19.1; *Sultanov*, 2024 WL 3520443; *Fox*, 2024 WL 3520767.[14]

Warrantless searches of electronic devices do not sufficiently advance the goals of the border-search exception, because the primary purpose of the border-search exception is customs enforcement: the interdiction of physical contraband and dutiable goods. A secondary purpose is preventing the entry of inadmissible persons. 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." SPA 21, ECF No. 19.1. 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

[14] *Fox* (No. 24-02262) is on appeal to this Court.

content on cell phones" or other electronic devices. *See Riley*, 573 U.S. at 386. Ultimately, travelers' extraordinary privacy interests outweigh any legitimate governmental interests. Therefore, border searches of electronic devices require a warrant based on probable cause. *See* SPA 29-30, ECF No. 19.1.

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." *Flores-Montano*, 541 U.S. at 154 n.2 (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 & n.18.

While no circuit court following *Riley* has yet held that a warrant is always required for border device searches, two circuits have required warrants in certain circumstances. In the Ninth Circuit, a warrant is required when a device search goes beyond the limited scope of searching for digital contraband. *See Cano*, 934 F.3d at 1007. In the Fourth Circuit, 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, deciding in the first instance, should 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." SPA 30, ECF No. 19.1. And although the challenged search in this case was a forensic search, *see* SPA 7, ECF No. 19.1, there is no basis for a different Fourth Amendment rule for manual searches, given how highly invasive they are.

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."

573 U.S. at 401. *See also United States v. McKenzie*, 13 F.4th 223, 228–29 (2d Cir. 2021) (officers obtained warrant to search car after several hours). The government has experience in obtaining warrants for searches of electronic devices and in other contexts at the border.[15]

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, as the district court noted. *See* SPA 19, ECF No. 19.1; *Riley*, 573 U.S. at 388, 391, 402. Border officers would still need probable cause, but could conduct a warrantless search of a device to protect against imminent harm. *See United States v. Caraballo*, 831 F.3d 95, 102 (2d Cir. 2016).

VI. Absent a Warrant, the Fourth Amendment Requires, at a Minimum, Reasonable Suspicion of Digital Contraband for Electronic Device Searches at the Border

If this Court declines to hold that border searches of electronic devices require a warrant, this Court should rule that all device searches—whether manual or forensic—must be supported by reasonable suspicion that the device contains digital

[15] *See* U.S. Dep't of Homeland Sec., *U.S. Border Patrol Digital Forensics Programs PIA* (Apr. 6, 2018) 1-2, https://perma.cc/HUY4-KWHD; U.S. Customs and Border Protection, *Personal Search Handbook* 37, 40 (2021), https://perma.cc/8GR9-T65S; 19 C.F.R. § 145.3 (b) (warrant required to open mail containing only correspondence).

contraband *and* be limited in scope to searching for digital contraband. Not only does this rule remain faithful to *Riley* and related Supreme Court cases, it is consistent with this Court's jurisprudence.

This rule extends that crafted by the Ninth Circuit in *Cano*, which held that all cell phone searches at the border must be limited in scope to searching for digital contraband. *Cano*, 934 F.3d 1007, 1019 (concluding that recording phone numbers in a call log is not related to digital contraband). Because binding *en banc* circuit precedent required reasonable suspicion for forensic, but not manual, searches, *Cano* also held that only forensic searches require reasonable suspicion that the device contains digital contraband. *Id.* at 1016 (citing *Cotterman*, 709 F.3d at 968). This Court is not so constrained. Though the instant case involves a challenge to forensic device searches, this Court should take this opportunity to protect the privacy of U.S. persons and other international travelers by extending the *Cano* rule to manual searches and rejecting the less privacy-protective approaches of the other circuits.[16] This Court has held that the reasonableness of a warrantless search depends on "the degree to which it intrudes upon an individual's privacy and … the degree to which it is needed for the promotion of legitimate governmental interests." *United States v. Miller*, 430 F.3d 93, 97 (2d Cir. 2005) (cleaned up). The extended *Cano* rule is

[16] *See Alasaad*, 988 F.3d 8; *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018); *United States v. Xiang*, 67 F.4th 895 (8th Cir. 2023); *United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018).

appropriate given that all device searches at the border amount to a severe privacy intrusion, outweighing any legitimate governmental interests.

First, device searches at the border—both manual and forensic—require at least reasonable suspicion. This Court has held that at the border, "[r]outine searches … do not substantially infringe on a traveler's privacy rights." *United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006). By contrast, "the level of intrusion into a person's privacy" is substantial for border device searches and so they are non-routine searches that require at least reasonable suspicion. *See id.* This Court should decline to make a distinction in the level of suspicion required between manual and forensic searches, given that manual searches can reveal the same highly sensitive private information as forensic searches and *Riley* involved a manual cell phone search. *See supra* Part III. In *Irving*, this Court upheld a manual search of computer diskettes because it was supported by reasonable suspicion. 452 F.3d at 124. In *Levy*, this Court upheld the copying of a traveler's paper notebook because it was supported by reasonable suspicion. 803 F.3d at 123. In both cases, this Court declined to decide whether these searches were non-routine. But today's electronic devices contain the equivalent of virtually innumerable notebooks and have exponentially larger storage capacities than diskettes had in 2006, making the privacy intrusion of any border device search substantial and requiring at least reasonable suspicion.

Second, limiting reasonable suspicion to whether the device contains digital contraband and limiting the scope to searching for digital contraband 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). These digital contraband limitations hew closely to the core purpose of the border-search exception, which is to find dutiable or prohibited goods themselves in the items to be searched. *See supra* Part IV. The Ninth Circuit recognized this fact, noting that "every border-search case the Supreme Court has decided involved searches to locate *items being smuggled* rather than evidence." *Cano*, 934 F.3d at 1018 (cleaned up). The Ninth Circuit thus rejected the notion that warrantless cell phone searches at the border may seek evidence of contraband that is not present at the border or evidence of other "border-related crimes." *Id.* In so holding, the Ninth Circuit explicitly departed from the Fourth Circuit's rule that allows forensic border device searches with individualized suspicion for "the prevention and disruption of ongoing efforts to export contraband illegally." *Id.* at 1017.

The Ninth Circuit also properly rejected the idea that warrantless border device searches may be used to gather evidence for general law enforcement, which is even further afield from the core purpose of the border-search exception. *See supra*

Part IV.B. The Ninth Circuit noted that the "distinction between seizing goods at the border because their importation is prohibited and seizing goods at the border because they may be useful in prosecuting crimes" dates back to the Supreme Court's decision in *Boyd*. *Cano*, 934 F.3d at 1018. More recently, the Supreme Court 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. Granting the government authority to search devices 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.

And for the reasons discussed above, *see supra* Part IV.B., this Court's conclusion in *Levy* that permitted copying a physical notebook for criminal investigative purposes does not dictate the rule for electronic devices, which are an entirely separate "category of effects." *Riley*, 573 U.S. at 386.

Finally, a rule requiring reasonable suspicion that a device contains digital contraband at the outset, and limiting device searches to digital contraband, is administrable. Law enforcement officers in many other warrantless search contexts are required to have reasonable suspicion. *See*, *e.g.*, *Gant*, 556 U.S. at 346; *Terry v. Ohio*, 392 U.S. 1, 30 (1968). Just as officers conducting *Terry* stops must be given training in how to seek weapons only, border officers can be trained to ensure their

device searches are for digital contraband only. Border officers are already familiar with the reasonable suspicion standard, including its application to search for only contraband. 19 C.F.R. § 145.3 (a)-(b) (requiring reasonable suspicion of contraband before international mail can be opened, and a warrant before reading correspondence).

CONCLUSION

Amici respectfully request that this Court hold that the Fourth Amendment requires border officers to obtain a warrant before conducting an electronic device search at the border, or at least have reasonable suspicion that the device contains digital contraband and limit their search to digital contraband.

November 22, 2024

Respectfully submitted,

Sophia Cope
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333 (phone)
(415) 436-9993 (fax)
sophia@eff.org

NEW YORK CIVIL LIBERTIES UNION FOUNDATION
Molly Biklen
125 Broad Street, 19th Floor
New York, N.Y. 10004
(212) 607-3300
mbiklen@nyclu.org

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

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7) and Federal Rule of Appellate Procedure 29(a)(5) because it contains 6,993 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 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.

/s/ Esha Bhandari
Esha Bhandari

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on November 22, 2024, I electronically filed the foregoing Brief of *Amici Curiae* with the Clerk of the Court for the United States Court of Appeals for the Second Circuit by using the appellate ACMS system. Participants in the case are registered ACMF users, and service will be accomplished by the appellate ACMF system.

/s/ Esha Bhandari
Esha Bhandari

Counsel for Amici Curiae