NO. 22-1801

IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE.

V.

HAITAO XIANG,

DEFENDANT-APPELLANT,

On Appeal from the United States District Court
for the Eastern District of Missouri
Case No. 4:19-cr-00980-HEA
The Honorable Henry Edward Autrey, United States District Court Judge

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

Esha Bhandari
Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: (212) 549-2500
Fax: (212) 549-2654
Email: ebhandari@aclu.org, nwessler@aclu.org

Hannah Zhao
Counsel of Record
Jennifer Pinsof
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993
Email: zhao@eff.org, jpinsof@eff.org

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

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

Dated: July 14, 2022

/s/ *Hannah Zhao*
Hannah Zhao

Counsel of Record for Amici Curiae

Appellate Case: 22-1801 Page: 2 Date Filed: 07/15/2022 Entry ID: 5177838

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT i

TABLE OF CONTENTS ii

TABLE OF AUTHORITIES iii

STATEMENT OF INTEREST OF AMICI 1

INTRODUCTION 2

ARGUMENT 4

I. THE FOURTH AMENDMENT REQUIRES A WARRANT FOR ELECTRONIC DEVICE SEARCHES AT THE BORDER 4

A. The Fourth Amendment Balancing Test in *Riley* Informs Whether the Border-Search Exception to the Warrant Requirement Applies to Electronic Devices 6

B. Warrantless Electronic Device Searches Are Highly Intrusive of Personal Privacy 7

C. Warrantless Electronic Device Searches Are Untethered from the Border-Search Exception's Purposes 12

II. THE FOURTH AMENDMENT REQUIRES AT LEAST REASONABLE SUSPICION OF DIGITAL CONTRABAND FOR ELECTRONIC DEVICE SEARCHES AT THE BORDER 16

CONCLUSION 18

CERTIFICATE OF COMPLIANCE WITH RULE 32 20

CERTIFICATE OF COMPLIANCE WITH EIGHTH CIRCUIT RULE 28A(h) 21

CERTIFICATE OF SERVICE 22

TABLE OF AUTHORITIES

Cases

Alasaad v. Nielsen,
419 F.Supp.3d 142, 158 (D. Mass. 2019), *aff'd in part*, *vacated in part*, *rev'd in part sub nom. Alasaad v. Mayorkas*, 988 F.3d 8 (1st Cir. 2021) 14, 18

Arizona v. Gant,
556 U.S. 332 (2015).....13

Boyd v. United States,
116 U.S. 616 (1886).....8

Carpenter v. United States,
138 S. Ct. 2206 (2018).....6

Carroll v. United States,
267 U.S. 132 (1925).....13

Kyllo v. United States,
533 U.S. 27 (2001).....6

United States v. Aigbekaen,
943 F.3d 713 (4th Cir. 2019) 15, 17

United States v. Cano,
934 F.3d 1002 (9th Cir. 2019) .....*passim*

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013) .....*passim*

United States v. Flores-Montano,
541 U.S. 149 (2004).....*passim*

United States v. Jones,
565 U.S. 400 (2012).....11

United States v. Kamaldoss,
2022 WL 1200776 (E.D.N.Y. Apr. 22, 2022) 6, 15

United States v. Kim,
103 F.Supp.3d 32 (D.D.C. 2015).....7, 15

Appellate Case: 22-1801 Page: 4 Date Filed: 07/15/2022 Entry ID: 5177838

United States v. Kolsuz,
890 F.3d 133 (4th Cir. 2018) 9, 17

United States v. Montoya de Hernandez,
473 U.S. 531 (1985).....5, 17

United States v. Ramsey,
431 U.S. 606 (1977).....5, 7, 13, 17

United States v. Saboonchi,
48 F. Supp. 3d 815 (D. Md. 2014) 9

United States v. Smasal,
2015 WL 4622246 (D. Minn. June 19, 2015).....17

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 6

United States v. Wurie,
728 F.3d 1 (1st Cir. 2013).....10

Other Authorities

Ericsson, *Ericsson Mobility Report* (June 2022).....8

Pew Research Center, *Mobile Fact Sheet* (April 7, 2021) 8

U.S. Customs and Border Protection, *Border Search of Electronic Devices, Directive No. 3340-049A* (Jan. 4, 2018) 9

U.S. Customs and Border Protection, *Immigration and Inspection Program* (Feb. 21, 2014).....14

Appellate Case: 22-1801 Page: 5 Date Filed: 07/15/2022 Entry ID: 5177838

STATEMENT OF INTEREST OF AMICI[1]

The Electronic Frontier Foundation ("EFF") is a member-supported, nonprofit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 35,000 members. EFF has done extensive work to highlight the unprecedented and significant threats to personal privacy posed by border searches of electronic devices, including representing plaintiffs in litigation and writing numerous amicus briefs, blog posts, and detailed reports.[2]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with approximately two million members and supporters dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The ACLU has served as counsel and as amicus in numerous cases considering the constitutionality of warrantless and suspicionless searches of electronic devices at the U.S. border.

---

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), *amici curiae* certify that no person or entity, other than *amici curiae*, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. The parties have consented to the filing of this brief.

[2] *See generally* https://www.eff.org/issues/border-searches.

INTRODUCTION

Digital is different. The Fourth Amendment's border-search exception to the warrant requirement, permitting certain warrantless and suspicionless searches of belongings and persons at the U.S. border, should not be extended to searches of electronic devices like those Mr. Xiang was carrying. All border searches of electronic devices fall outside the border-search exception. This is because *any* search of digital data is a "highly intrusive" search that impacts the "dignity and privacy interests" of the traveler. *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). Following the Supreme Court's reasoning in *Riley v. California*, 573 U.S. 373 (2014), border officers should be required to obtain a probable-cause warrant to search the data stored on a digital device.

The *Riley* Court explained that, in determining whether to apply an existing warrant exception to a "particular category of effects" such as cell phones, individual privacy interests must be balanced against legitimate governmental interests. *Id*. at 386. The government's interests are analyzed by considering whether warrantless, suspicionless searches of a particular category of property are sufficiently "tethered" to the purposes underlying the exception. *Id*. In the case of digital data, warrantless and suspicionless searches of electronic devices at the border are not sufficiently "tethered" to the narrow purposes justifying the border-

Appellate Case: 22-1801 Page: 7 Date Filed: 07/15/2022 Entry ID: 5177838

search exception: immigration and customs enforcement. That is, these searches are not necessary to, and do not sufficiently advance, those goals.

Moreover, even if warrantless searches of digital data were meaningfully tethered to the purposes justifying the exception, the unprecedented privacy interests that travelers have in their electronic devices outweigh any legitimate governmental interests in conducting the searches. Individual privacy interests are at their zenith in devices such as cell phones and laptops, even at the border. Prior to the rise of mobile computing, the "amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile." *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (en banc). Today, however, the "sum of an individual's private life" sits in the pocket or purse of any traveler carrying a cell phone, laptop, or other electronic device. *Riley*, 573 U.S. at 394.

In this case, the district court erred in denying Mr. Xiang's motion to suppress evidence gathered from a search of his electronic devices. Mr. Xiang's initial stop and search at O'Hare Airport was not based on any independent suspicion by the border officer, but was based on a pre-existing investigation initiated by Monsanto and the FBI. ECF 117 (R. & R.) at 4. The FBI failed to seek a warrant, as would have been required to search Mr. Xiang's devices if he were not physically at the border. Instead, all his electronic devices were seized at the

Appellate Case: 22-1801 Page: 8 Date Filed: 07/15/2022 Entry ID: 5177838

airport, and then imaged (copied in whole) and searched ten days later. *Id.* at 7–8. Under these circumstances, the district court determined that the search of Mr. Xiang's devices fell within the border-search exception.

But a "person's digital life ought not to be hijacked simply by crossing a border." *Cotterman*, 709 F.3d at 965. This Court has an opportunity to clarify what Fourth Amendment standards apply to electronic device searches at the border. It should hold that, consistent with *Riley*, border searches of electronic devices require a warrant based on probable cause.

Should this Court decline to require a warrant, it should hold that the Constitution requires at least reasonable suspicion that a device contains digital contraband for any search of the device's digital content. Any less stringent rule risks eviscerating travelers' privacy rights whenever they cross the border.

ARGUMENT

I. THE FOURTH AMENDMENT REQUIRES A WARRANT FOR ELECTRONIC DEVICE SEARCHES AT THE BORDER

Because the Supreme Court prefers "clear guidance" and "categorical rules," *Riley*, 573 U.S. at 398, this Court should adopt the clear rule that all border searches of data stored on electronic devices require a warrant based on probable

Appellate Case: 22-1801 Page: 9 Date Filed: 07/15/2022 Entry ID: 5177838

cause.[3] Notably, *Riley* rejected the lower standard of reasonable suspicion for cell phone searches incident to arrest, and required a probable-cause warrant instead. *Id*. at 398–99.

The Supreme Court has never held that reasonable suspicion is a ceiling for every border search, or that property searches at the border can never require heightened protection. Rather, the Supreme Court has left open the possibility that certain types of border searches may be subjected to a higher standard than reasonable suspicion. *See Flores-Montano*, 541 U.S. at 152; *United States v. Ramsey*, 431 U.S. 606, 623–24 n.18 (1977) (leaving open the possibility that where border searches burden First Amendment rights, the "full panoply" of Fourth Amendment protections might apply). In fact, the Court's border search decisions suggest that reasonable suspicion is the *floor* for highly invasive border searches. *See United States v. Montoya de Hernandez,* 473 U.S. 531, 541 n.4 (1985) (declining to decide "what level of suspicion" is required for highly intrusive searches); *Flores-Montano*, 541 U.S. at 154 n.2 (quoting *Ramsey*, 431 U.S. at 618 n.13); *cf. United States v. Kamaldoss*, 2022 WL 1200776, at *9 (E.D.N.Y. Apr. 22,

[3] A warrant should not be difficult to obtain at the border. "Recent technological advances . . . have . . . made the process of obtaining a warrant itself more efficient." *Riley*, 573 U.S. at 401. Border officers clearly know how to obtain judicial authorization for certain searches and seizures. *See, e.g.*, *Montoya de Hernandez*, 473 U.S. at 535 ("[C]ustoms officials sought a court order authorizing a pregnancy test, an [x-ray], and a rectal examination.").

Appellate Case: 22-1801 Page: 10 Date Filed: 07/15/2022 Entry ID: 5177838

2022) (recognizing that "[w]hile the Supreme Court has not spoken to the precise circumstances under which some level of suspicion is required for a border search, it has suggested that 'in the case of highly intrusive searches' where salient 'dignity and privacy interests' are at stake, 'a requirement of . . . suspicion' might be supported." (citing *Flores-Montano*, 541 U.S. at 152)).

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

The Supreme Court has cautioned that new technologies should not be allowed to "erode the privacy guaranteed by the Fourth Amendment." *Kyllo v. United States*, 533 U.S. 27, 34 (2001); *see also Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) ("As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.") (internal quotations and citation omitted); *cf. United States v. Warshak*, 631 F.3d 266, 285 (6th Cir. 2010) ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."). This is true regardless of whether the warrantless search of electronic devices was conducted pursuant to the search-incident-to-arrest exception or the border-search exception.

Appellate Case: 22-1801 Page: 11 Date Filed: 07/15/2022 Entry ID: 5177838

The *Riley* Court's analytical framework for whether a warrantless device search properly fell within the search-incident-to-arrest exception is instructive for the border-search exception as well.[4] In determining whether to apply an existing warrant exception to a "particular category of effects," individual privacy interests must be balanced against legitimate governmental interests. 573 U.S. at 385–86. In the case of border searches of digital devices, this balancing weighs in favor of the traveler.

B. Warrantless Electronic Device Searches Are Highly Intrusive of Personal Privacy

Before the digital revolution, border searches of personal property, like searches incident to arrest, were "limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy." *Riley*, 573 U.S. at 393. In *Riley*, the government argued that a search of cell phone data, like a search of physical items, should fall within the search-incident-to-arrest exception and obviate a warrant requirement. *Id*. The Court rejected this argument: "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Id*.; *see also United States v. Kim*, 103 F.Supp.3d 32, 55 (D.D.C. 2015) (in a border search case, stating *Riley* "strongly indicate[d] that a digital data storage

[4] The Supreme Court has recognized that while the specific purposes of the two exceptions to the warrant requirement differ, the border-search exception "is like the similar 'search incident to lawful arrest' exception." *Ramsey*, 431 U.S. at 621.

Appellate Case: 22-1801 Page: 12 Date Filed: 07/15/2022 Entry ID: 5177838

device cannot fairly be compared to an ordinary container when evaluating the privacy concerns involved"). The Court examined the nature of cell phones and concluded they are "not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" *Riley*, 573 U.S. at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

Privacy interests in protecting electronic devices from warrantless and suspicionless intrusions are heightened due to the ubiquity of these devices. Most people carry electronic devices everywhere they go. Cell phones in particular have become "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley*, 573 U.S. at 385. Globally, there are 8.2 billion cell phone subscriptions, including 6.3 billion for a smartphone.[5] Ninety-seven percent of American adults own a cell phone, with 85 percent owning a smartphone.[6] Additionally, 77 percent own a laptop or desktop computer.[7] "Prior to the digital age, people did not

---

[5] Ericsson, *Ericsson Mobility Report* (June 2022), at 5, https://www.ericsson.com/49d3a0/assets/local/reports-papers/mobility-report/documents/2022/ericsson-mobility-report-june-2022.pdf.

[6] Pew Research Center, *Mobile Fact Sheet* (April 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/.

[7] *Id*.

Appellate Case: 22-1801 Page: 13 Date Filed: 07/15/2022 Entry ID: 5177838

typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception." *Riley*, 573 U.S. at 395.[8]

Electronic devices differ fundamentally—quantitatively and qualitatively—from physical containers like luggage. *Id*. at 393.

Quantitatively, "the sheer quantity of information available on a cell phone makes it unlike other objects to be searched." *United States v. Saboonchi*, 48 F. Supp. 3d 815, 819 (D. Md. 2014); *see also United States v. Kolsuz*, 890 F.3d 133, 145 (4th Cir. 2018) ("The sheer quantity of data stored on smartphones and other digital devices dwarfs the amount of personal information that can be carried over a border . . . in luggage or a car."). With their "immense storage capacity," electronic devices can contain "millions of pages of text, thousands of pictures, or hundreds of videos." *Riley*, 573 U.S. at 393–94; *see also Cotterman*, 709 F.3d at 964 ("The average 400-gigabyte laptop hard drive can store over 200 million pages—the equivalent of five floors of a typical academic library.").

[8] Other types of portable electronic devices raise equivalent concerns. *See* U.S. Customs and Border Protection, *Border Search of Electronic Devices, Directive No. 3340-049A* (Jan. 4, 2018), § 3.2 (broadly defining "electronic device" as "[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, cameras, music and other media players."), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.

Appellate Case: 22-1801 Page: 14 Date Filed: 07/15/2022 Entry ID: 5177838

Qualitatively, electronic devices contain information "of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records." *United States v. Wurie*, 728 F.3d 1, 8 (1st Cir. 2013), *aff'd*, *Riley*, 573 U.S. 373. And they "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 data reveals a detailed account of an individual's political affiliations, religious beliefs and practices, sexual and romantic life, financial situation, health conditions, and family and professional associations. *Id.* at 395–96. Electronic devices thus "are simultaneously offices and personal diaries" and "contain the most intimate details of our lives." *Cotterman*, 709 F.3d at 964; *accord United States v. Cano*, 934 F.3d 1002, 1015 (9th Cir. 2019).

Today's electronic devices enable the reconstruction of "the sum of an individual's private life" covering a lengthy amount of time—"back to the purchase of the [device], or even earlier." *Riley*, 573 U.S. at 394; *accord Cano*, 934 F.3d at 1020. While people cannot physically "lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read," they can now do so digitally. *Riley*, 573 U.S. at 393; *see also Cotterman*, 709 F.3d at 965 (stating "digital devices allow us to carry

Appellate Case: 22-1801 Page: 15 Date Filed: 07/15/2022 Entry ID: 5177838

the very papers we once stored at home"). But it is not just that a cell phone "contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Riley*, 573 U.S. at 396–97. Historic location information, for example, "is a standard feature on many smartphones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Id.* at 396 (citing *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). Such detailed, highly sensitive data has no analogue in pre-digital searches because it never could have been carried with a person, or never existed at all.

Given the vast amounts of highly personal information that electronic devices contain, even manual searches not involving special training or equipment can greatly burden privacy interests. A border officer can easily open and peruse myriad stored files, programs, and apps, and do so with a device's own built-in search function, allowing the officer to search for particular words and images. The data that can be accessed manually can reveal a wealth of sensitive personal information, including prescription information, employment, travel history, and browsing history, as well as metadata, such as the date/time associated with the content, usage history, sender and receiver information, or location data. In *Riley*, that a manual search *could* reveal the massive amount of information on a device

was enough for the Supreme Court to rule that a warrant was required. *See* 573 U.S. at 379–80, 393–97.

In sum, because electronic devices differ categorically from luggage and other physical items that travelers carry across the border, border searches of electronic devices have extraordinary privacy implications. And these privacy implications are only increasing as technology continues to advance. As the volume and types of data devices contain continue to grow, so does the ease with which law enforcement can quickly search them. *See Riley*, 573 U.S. at 394 ("We expect that the gulf between physical practicability [of searching analog containers] and digital capacity [of electronic devices] will only continue to widen in the future."). Thus, the privacy interests travelers have in their electronic devices today are even greater than those considered in *Riley*.

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

None of the exceptions to the Fourth Amendment warrant requirement—including search incident to arrest (as was the case in *Riley*) and border search (as is the case here)—apply automatically upon invocation. Rather, warrantless, suspicionless searches of electronic devices at the border must be sufficiently "tethered" to the narrow purposes justifying the border-search exception: immigration and customs enforcement. *See Cano*, 934 F.3d at 1013 ("[T]he Supreme Court has identified two principal purposes behind warrantless border

searches: First to identify '[t]ravellers . . . entitled to come in' and, second, to verify their 'belongings as effects which may be lawfully brought in.'") (quoting *Carroll v. United States*, 267 U.S. 132, 154 (1925)); *see also Arizona v. Gant*, 556 U.S. 332, 343 (2015) (holding that the search-incident-to-arrest exception does not permit all warrantless searches; rather, the search must be "[]tether[ed]" to "the justifications underlying the . . . exception"). As with the search-incident-to-arrest exception, the border-search exception is supposed to "strike[ ] the appropriate balance in the context of physical objects, [but] neither of its rationales has much force with respect to digital content on cell phones" or other electronic devices. *Riley*, 573 U.S. at 386.

First, warrantless border searches of electronic devices are not sufficiently tethered to customs enforcement. The customs rationale is meant to regulate the physical items entering the country. As the Supreme Court explained in *United States v. Ramsey*, "[t]he border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country." 431 U.S. at 620. As such, the customs rationale of the border-search exception aims to regulate the flow of physical items, typically because the items were not properly declared for duty or are contraband.

Similarly, warrantless border searches of electronic devices are not

Appellate Case: 22-1801 Page: 18 Date Filed: 07/15/2022 Entry ID: 5177838

sufficiently tethered to preventing the entry of inadmissible persons. Border officers determine a traveler's immigration status and authority to enter the United States by questioning travelers and inspecting official documents such as passports and visas. The government need not have warrantless access to travelers' electronic devices in order to prevent the entry of inadmissible persons. *See Alasaad v. Nielsen*, 419 F.Supp.3d 142, 158 (D. Mass. 2019), *aff'd in part*, *vacated in part*, *rev'd in part sub nom. Alasaad v. Mayorkas*, 988 F.3d 8 (1st Cir. 2021) (rejecting government's argument that it needs suspicionless and unbounded access to travelers' electronic devices in order to prevent the entry of inadmissible persons, particularly when those travelers are U.S. citizens and lawful permanent residents who are automatically admissible).[9] The government has even less need for this information when the individual is leaving the United States.

In addition, gathering evidence for general law enforcement is completely untethered from the border-search exception's permissible purposes. *See Cano*, 943 F.3d at 1016 (searches not for digital contraband but "for evidence of a crime . . . exceed[] the proper scope of a border search"). The government's interest in finding evidence of crime or other violations of law is no greater at the border than

[9] U.S. Customs and Border Protection, *Immigration and Inspection Program* (Feb. 21, 2014) ("U.S. citizens are automatically admitted upon verification of citizenship; aliens are questioned and their documents are examined to determine admissibility"), https://www.cbp.gov/border-security/ports-entry/overview.

Appellate Case: 22-1801 Page: 19 Date Filed: 07/15/2022 Entry ID: 5177838

anywhere else. Yet here, the border searches of electronic devices were conducted to advance a pre-existing FBI investigation. Under similar circumstances, the Fourth Circuit in *United States v. Aigbekaen* required a warrant for a device search at the border. 943 F.3d 713, 722–23 (4th Cir. 2019); *see also Kamaldoss*, 2022 WL 1200776, at *11 ("a warrantless forensic search may not be justified by the government's 'generalized interest in law enforcement and combatting crime'") (citing *Aigbekaen*, 943 F.3d at 721); *Kim*, 103 F.Supp.3d at 59 (ordering suppression of evidence from a laptop search "for the purpose of gathering evidence in a pre-existing investigation," because the search "was so invasive of Kim's privacy and so disconnected from . . . the considerations underlying the breadth of the government's authority to search at the border").

Here, federal law enforcement investigating Mr. Xiang could have sought a warrant, but declined to do so. Instead, they contacted border officers, knowing Mr. Xiang had plans to travel internationally. Rather than being tethered to the immigration and customs purpose of a border search, the purpose of this border search was to facilitate a warrantless search for evidence. But a "person's digital life ought not to be hijacked simply by crossing a border." *Cotterman*, 709 F.3d at 965.

Ultimately, even if the Court believes searches of electronic devices are not completely untethered from the purposes of the border-search exception, the

Appellate Case: 22-1801 Page: 20 Date Filed: 07/15/2022 Entry ID: 5177838

extraordinary privacy interests that travelers have in their electronic devices, *see supra* Part I.B, still outweigh any legitimate governmental interests. Governmental interests do "not justify dispensing with the warrant requirement across the board." *Riley*, 573 U.S. at 388. In short, "some searches, even when conducted within the scope of the [border-search] exception, are so *intrusive* that they require additional justification, up to and including probable cause and a warrant." *Cano*, 934 F.3d at 1011 (emphasis in original).

II. THE FOURTH AMENDMENT REQUIRES AT LEAST REASONABLE SUSPICION OF DIGITAL CONTRABAND FOR ELECTRONIC DEVICE SEARCHES AT THE BORDER

Should this Court decline to require a warrant for electronic device searches at the border, it should find that such searches require reasonable suspicion that the device contains digital contraband. The district court in this case "presume[d], without deciding, that the search at issue was a forensic or advanced search that required a showing of reasonable suspicion[.]" ECF 117 (R. & R.) at 25; ECF 130 (Op., Mem., & Order) at 1 (adopting R. & R. "in its entirety as the opinion of the Court"). But travelers' extraordinary privacy interests in their digital data render *all* device searches—whether forensic or manual—"non-routine" border searches requiring at least reasonable suspicion.

"Non-routine" border searches require at least reasonable suspicion. *See Flores-Montano*, 541 U.S. at 152; *see also United States v. Oyekan*, 786 F.2d 832,

Appellate Case: 22-1801 Page: 21 Date Filed: 07/15/2022 Entry ID: 5177838

836 (8th Cir. 1986) (non-routine border searches require "'particularized and objective basis for suspecting the particular person' of smuggling" (citing *Montoya de Hernandez*, 473 U.S. at 541)). The Supreme Court has defined "non-routine" border searches as those that are "highly intrusive" and impact the "dignity and privacy interests" of travelers. *Flores-Montano*, 541 U.S. at 152; *accord Cano*, 934 F.3d at 1012; *Aigbekaen*, 943 F.3d at 720. Searches carried out in a "particularly offensive manner" can also be non-routine. *Ramsey*, 431 U.S. at 618 n.13; *see also Kolsuz*, 890 F.3d at 138.

At minimum, this Court should hold that electronic device searches are non-routine border searches that require reasonable suspicion. Even property searches may be non-routine if they are offensively intrusive. *Cf. United States v. Smasal*, 2015 WL 4622246, at *6 (D. Minn. June 19, 2015) (noting that "drilling holes into various objects" are non-routine). Due to the extraordinary quantity and breadth of personal information electronic devices can reveal, *see supra* Part I.B, their search rises to the level of "highly intrusive" searches that impact the "dignity and privacy interests" of travelers, and are consequently non-routine, *Flores-Montano*, 541 U.S. at 152, 154 n.2.

Furthermore, reasonable suspicion must address the presence of digital contraband itself—rather than evidence of a crime or other violations of law—because device searches must be "tethered" to the narrow purposes of the border-

Appellate Case: 22-1801 Page: 22 Date Filed: 07/15/2022 Entry ID: 5177838

search exception: determining the admissibility of goods and people. *See supra* Part I.C; *see also Riley*, 573 U.S. at 386. This Court should follow the Ninth Circuit in ruling that electronic device searches at the border, "whether manual or forensic, must be limited in scope to a search for digital contraband." *Cano*, 934 F.3d 1002, 1007 (9th Cir. 2019); *cf. Alasaad*, 419 F.Supp.3d at 166–67, *aff'd in part, vacated in part, rev'd in part*, 988 F.3d 8 (1st Cir. 2021) (holding on summary judgment that for both manual and forensic searches, the Fourth Amendment requires border officers to have reasonable suspicion that an electronic device contains digital contraband).

In sum, travelers' extraordinary privacy interests in their digital data render all device searches "non-routine" border searches requiring at least reasonable suspicion of digital contraband.

CONCLUSION

For the reasons stated above, this Court should adopt the categorical rule that all border searches of electronic devices require a warrant or, alternatively, that reasonable suspicion of digital contraband is required.

Dated: July 14, 2022

By: /s/ *Hannah Zhao*
Hannah Zhao
Counsel of Record
Jennifer Pinsof
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street

Appellate Case: 22-1801 Page: 23 Date Filed: 07/15/2022 Entry ID: 5177838

San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993
Email: zhao@eff.org, jpinsof@eff.org

Esha Bhandari
Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: (212) 549-2500
Fax: (212) 549-2654
Email: ebhandari@aclu.org, nwessler@aclu.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE WITH RULE 32

Pursuant to Fed. R. App. P. 32(g), I certify as follows:

1. This Brief of Amici Curiae Electronic Frontier Foundation and American Civil Liberties Union in Support of Defendant-Appellant complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 4,060 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 365, the word processing system used to prepare the brief, in 14 point Times New Roman font.

Dated: July 15, 2022

/s/ *Hannah Zhao*
Hannah Zhao

Counsel of Record for Amici Curiae

Appellate Case: 22-1801 Page: 25 Date Filed: 07/15/2022 Entry ID: 5177838

CERTIFICATE OF COMPLIANCE WITH EIGHTH CIRCUIT RULE 28A(h)

Pursuant to this Court's Rule 28A(h), I hereby certify that the electronic version of this Brief of Amici Curiae Electronic Frontier Foundation and American Civil Liberties Union in Support of Defendant-Appellant has been scanned for viruses and is virus-free.

Dated: July 15, 2022

/s/ *Hannah Zhao*
Hannah Zhao

Counsel of Record for Amici Curiae

Appellate Case: 22-1801 Page: 26 Date Filed: 07/15/2022 Entry ID: 5177838

CERTIFICATE OF SERVICE

I hereby certify that on July 14, 2022, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Eighth Circuit by using the CM/ECF system.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system, pursuant to Eighth Circuit Rule 25A.

Dated: July 14, 2022

/s/ *Hannah Zhao*
Hannah Zhao

Counsel of Record for Amici Curiae

Appellate Case: 22-1801 Page: 27 Date Filed: 07/15/2022 Entry ID: 5177838