Nos. 20-1077, 20-1081

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

GHASSAN ALASAAD; NADIA ALASAAD; SUHAIB ALLABABIDI; SIDD BIKKANNAVAR; JÉRÉMIE DUPIN; AARON GACH; ISMAIL ABDEL-RASOUL aka ISMA'IL KUSHKUSH; DIANE MAYE ZORRI; ZAINAB MERCHANT; MOHAMMED AKRAM SHIBLY; MATTHEW WRIGHT,

Plaintiffs-Appellees/Cross-Appellants,

v.

CHAD F. WOLF, Acting Secretary of the U.S. Department of Homeland Security, in his official capacity; MARK A. MORGAN, Acting Commissioner of U.S. Customs and Border Protection, in his official capacity; MATTHEW T. ALBENCE, Acting Director of U.S. Immigration and Customs Enforcement, in his official capacity,

Defendants-Appellants/Cross-Appellees.

On Appeal from the United States District Court for the District of Massachusetts

PLAINTIFFS-APPELLEES'/CROSS-APPELLANTS' PRINCIPAL AND RESPONSE BRIEF

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

Esha Bhandari
Hugh Handeyside
Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street,
18th Floor
New York, NY 10004
(212) 549-2500 (phone)
(212) 549-2583 (fax)
ebhandari@aclu.org
hhandeyside@aclu.org
nwessler@aclu.org

Matthew R. Segal
BBO #654489
Jessie J. Rossman
BBO #670685
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MASSACHUSETTS, INC.
211 Congress Street
Boston, MA 02110
(617) 482-3170 (phone)
(617) 451-0009 (fax)
msegal@aclum.org
jrossman@aclum.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Rules

Other Authorities

INTRODUCTION

This case concerns the constitutional rights of individuals every time they cross the U.S. border. Border officers searched the smartphones, laptops, and other electronic devices of more than 40,000 international travelers in fiscal year 2019, an eight-fold increase compared to fiscal year 2012. Each of these searches invades someone's private life and raises especially acute concerns for the journalists, lawyers, medical professionals, and others who carry particularly sensitive information about their news sources, clients, and patients. Yet the U.S. government expressly authorizes border officers to conduct these searches without a warrant or probable cause, and usually without even reasonable suspicion. Defendants' policies and related practices transform the border into a digital dragnet where they can search and retain troves of highly personal information about individuals and their families, friends, and colleagues virtually without constraint.

Defendants' policies violate both the Fourth and First Amendments to the U.S. Constitution. Today's electronic devices contain vast quantities of highly personal information that the Supreme Court has repeatedly held requires a warrant to be searched in other contexts. *See Riley v. California*, 573 U.S. 373 (2014); *Carpenter v. United States*, 138 S. Ct. 2206 (2018). As in those contexts, searches of travelers' electronic devices at the border deeply intrude upon our "privacies of

life." *See Riley*, 573 U.S. at 403. Because warrantless searches of such devices at the border are not sufficiently tethered to the rationales underlying the border-search exception to the warrant requirement, *see id.* at 385–86, this Court should hold that the Constitution requires a warrant before electronic devices may be searched at the border. Should this Court decline to require a warrant, it should affirm the district court, which held 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.

REASONS WHY ORAL ARGUMENT SHOULD BE HEARD

This Court should hear oral argument in these cross-appeals, which present important constitutional questions of widespread importance for the rights of international travelers.

STATEMENT OF JURISDICTION

Plaintiffs-Appellees/Cross-Appellants ("Plaintiffs") agree with Defendants-Appellants'/Cross-Appellees' ("Defendants") Statement of Jurisdiction. *See* Corr. Appellants' Principal Br. ("Defs.' Br.") 10.

STATEMENT OF THE ISSUES

I. Do the government's policies permitting warrantless and usually suspicionless searches of electronic devices at the border violate the Fourth Amendment and, if so, does the Fourth Amendment instead require a warrant supported by probable cause (as Plaintiffs contend) or reasonable suspicion that the devices contain digital contraband for any type of digital search (as the district court held)?

II. Do the government's policies concerning searches of electronic devices at the border violate the First Amendment?

III. Do the government's policies permitting seizing and retaining a device after a traveler leaves the border ("long-term seizures") violate the Fourth Amendment because they do not require probable cause (or at least reasonable suspicion) at inception, and because they allow seizures of indefinite duration?

IV. In light of its holding that Plaintiffs' constitutional rights had been violated, did the district court err by declining to order the expungement of information unconstitutionally collected from them and retained by the government?

V. Did the district court correctly hold that Plaintiffs have injunctive standing?

STATEMENT OF THE CASE

This case involves a constitutional challenge by ten U.S. citizens and one lawful permanent resident to the policies and practices regarding border searches and long-term seizures of electronic devices by U.S. Customs and Border Protection ("CBP") and U.S. Immigration and Customs Enforcement ("ICE").

I. Facts

A. CBP's and ICE's Policies

CBP Directive No. 3340-049A (2018) ("CPB Policy") governs the agency's searches and long-term seizures of electronic devices at the border. SUMF ¶ 6.[1] It distinguishes between "basic" and "advanced" searches. In an advanced search, an officer connects external equipment to a traveler's device, with a wired or wireless connection, to access, review, copy, and/or analyze the contents of the device. *Id.* ¶ 7. In a basic search, an officer reviews the contents of a device without using external equipment. *Id.* ¶ 8. The CBP Policy permits officers to conduct basic searches without any suspicion. *Id.* ¶ 10. It permits officers to conduct advanced searches with "reasonable suspicion of activity in violation of the laws enforced or

[1] All cites in this brief to "SUMF" refer to Appendix ("App.") 279–351, Pls.' Reply in Supp. of Pls.' Stmt. of Undisputed Material Facts, D. Ct. Dkt. 99-1; and App. 352–53 (¶ 125.1), Pls.' Suppl. Stmt. of Undisputed Material Facts, D. Ct. Dkt. 103-1.

administered by CBP," except where there is a "national security concern," in which case officers need no suspicion to conduct an advanced search. *Id.* ¶ 9.

The CBP Policy prohibits officers from accessing "information that is solely stored remotely." Addendum 55 § 5.1.2. However, CBP officers can still view on an electronic device "cached" information that originated on the internet. SUMF ¶ 75.

The CBP Policy allows officers to seize and retain a device for search after a traveler leaves the border. *Id.* ¶ 11. These searches "'ordinarily' should not exceed five days," but can be prolonged with supervisory approval based on "extenuating circumstances." *Id.* The CBP Policy places no ultimate limit on a long-term seizure. *Id.* ¶ 12.

The CBP Policy permits retention of information from a traveler's device that is related to immigration, customs, and other enforcement matters. *Id.* ¶ 13. It also allows officers to share this information with federal, state, local, and foreign law enforcement agencies. *Id.* ¶ 14.

ICE Directive No. 7-6.1 (2009), also known as ICE Policy 10044.1, as superseded in part by an ICE Broadcast (2018) (together, "ICE Policy"), governs the agency's searches and long-term seizures of electronic devices at the border. SUMF ¶ 17. Like the CBP Policy, it allows basic searches without any suspicion

and advanced searches with reasonable suspicion. *Id.* ¶¶ 18–19. However, the ICE Policy does not have a "national security concern" exception. *See id.* ¶ 18.

The ICE Policy allows officers to seize and retain a device for search after a traveler leaves the border. *Id.* ¶ 21. The policy states that these searches should generally be completed within 30 days, but officers can prolong a device's detention with supervisory approval. *Id.*

Like the CBP Policy, the ICE Policy permits the agency to retain from a traveler's device information related to immigration, customs, and other enforcement matters. *Id.* ¶ 22. It also allows officers to share this information with federal, state, local, and foreign law enforcement agencies. *Id.* ¶ 24.

B. Frequency of Border Searches and Seizures of Electronic Devices

The number of border searches of travelers' devices is increasing rapidly. According to CBP, the agency searched 40,913 devices in fiscal year 2019,[2] a more than 22 percent increase from fiscal year 2018 (33,296) and up more than eight-fold from fiscal year 2012 (5,085). SUMF ¶ 52. Due to lapses in record-keeping, these CBP figures are undercounts. *See id.* ¶¶ 59–62. CBP also has reported

[2] *CBP Statement on Border Search of Electronic Devices* (Oct. 30, 2019), https://www.cbp.gov/newsroom/speeches-and-statements/cbp-statement-border-search-electronic-devices. Plaintiffs request that this Court take judicial notice of the data in Defendant's published report. *See* Fed. R. Evid. 201.

hundreds of long-term seizures of travelers' electronic devices in the last several years. *Id.* ¶ 55.

While ICE conducts hundreds of advanced searches each year, it does not maintain records of basic searches or long-term seizures of travelers' electronic devices. App. 251 ¶ 15 (Joint Stmt. Stip. Facts); SUMF ¶¶ 56, 58.

C. Magnitude and Sensitivity of Content in Electronic Devices

Electronic devices carried by travelers, such as smartphones or laptops, can contain a very large volume of information. SUMF ¶ 63. Travelers carry electronic devices that contain many different kinds of information, such as photos, contacts, emails, and text messages, and the devices may reveal such things as prescription information, travel history, and browsing history. *Id.* ¶ 64. Separate from the primary content stored on them, some electronic devices may also store metadata related to that content, such as the date and time associated with the content, usage history, sender and receiver information, or location data. *Id.* ¶ 69. That content may be revealed during a basic search, depending on the type of device, the operating system, the relevant settings, and the applications used to create and/or maintain the data. *Id.*

D. Legal Authority Claimed by CBP and ICE

CBP and ICE claim broad authority to search travelers' devices for general law enforcement purposes, far beyond violations of customs and immigration laws.

Id. ¶¶ 82–83. This includes "hundreds" of federal laws, including tax, bankruptcy, environmental, and consumer protection laws. *Id.* ¶¶ 81, 84. Defendants also assert interests in intelligence gathering and advancing pre-existing investigations. *Id.* ¶¶ 86, 91. Further, Defendants search devices at the request of other agencies. *Id.* ¶¶ 87–88. They even claim legal authority to search electronic devices when the subject of interest is not the traveler—such as when a traveler is a U.S. citizen and ICE seeks information about an immigrant relative or associate; when the traveler is a journalist or scholar with foreign sources of interest to the government; or when the traveler and investigative subject are business partners. *Id.* ¶¶ 89–90.

E. Plaintiffs

Plaintiffs are ten U.S. citizens and one lawful permanent resident: a limousine driver, a nursing student, the operator of a security technology business, a NASA engineer, two journalists, an artist, the editor of a media organization, a filmmaker, a computer programmer, and a professor who formerly served as an Air Force captain. All were subjected to searches of their electronic devices at the border. SUMF ¶¶ 120–149. Five were searched on multiple occasions. *Id.* ¶¶ 121, 123, 125, 125.1, 129, 130, 134–35, 137, 140–42. Two were searched after filing this lawsuit. *Id.* ¶¶ 125.1, 140–42.

These searches exposed sensitive information. For example, Plaintiffs Zainab Merchant and Nadia Alasaad objected to male CBP officers searching their

devices because they contained images showing both Plaintiffs without their headscarves, which they wear in public in accordance with their religious beliefs. *Id.* ¶¶ 122, 139. A CBP officer also viewed privileged communications between Merchant and one of her attorneys in this case. *Id.* ¶ 142. Further, several Plaintiffs use their devices for sensitive work; for example, Jérémie Dupin uses his searched device for his journalism work. *Id.* ¶ 129.

Defendants retain information that border officers observed during searches of seven Plaintiffs' phones. *Id.* ¶ 150.

Defendants seized and retained four Plaintiffs' electronic devices. *Id.* ¶¶ 152, 156, 162. These long-term seizures were of varying duration—12 days, 56 days, two months, and ten months. *Id.* ¶¶ 154, 160, 161, 166.

II. Prior Proceedings

On May 9, 2018, the district court denied Defendants' motion to dismiss. It held that Plaintiffs had plausibly asserted standing to seek injunctive and declaratory relief, as well as expungement, App. 86–96; plausibly stated Fourth Amendment claims against Defendants' policies on border device searches, *id.* 97–115, and long-term seizures, *id.* 115–16; and plausibly stated a First Amendment claim. *Id.* 121.

On November 12, 2019, the district court granted in part Plaintiffs' motion for summary judgment. Addendum 2–49. It held that Plaintiffs have standing for

both prospective relief and expungement, *id.* 8–15, and that suspicionless searches of electronic devices at the border violate the Fourth Amendment. *Id.* 15–39. Relying on *Riley*, the court held that all device searches—whether basic or advanced—implicate the same privacy interests and require reasonable suspicion that a device contains digital contraband. Addendum 30. The court exempted "cursory" searches, meaning a brief look to determine a device is operational and contains data, and that the person carrying it owns it. *Id.* 3, 31, 48. The court rejected Plaintiffs' argument that the Constitution requires a warrant for device searches. *Id.* 39.

As to Plaintiffs' Fourth Amendment claim regarding long-term seizures, the court held any seizure "must be for a reasonable period that allows for an investigatory search for contraband." *Id.* 43. The court did not address Plaintiffs' second seizure claim: that the Fourth Amendment requires the same standard of suspicion at the inception of the seizure as for the search, i.e., probable cause or at least reasonable suspicion.

The court denied both parties' motions for summary judgment on Plaintiffs' First Amendment claim to the extent that the claim "seeks some further ruling or relief based upon Plaintiffs' invocation of First Amendment rights, not otherwise granted" as to Plaintiffs' Fourth Amendment search claim. *Id.* 41–42.

The court granted declaratory relief, stating:

> [T]he CBP and ICE policies for 'basic' and 'advanced' searches, as presently defined, violate the Fourth Amendment to the extent that the policies do not require reasonable suspicion that the devices contain contraband for both such classes of non-cursory searches and/or seizure of electronic devices; and that the non-cursory searches and/or seizures of Plaintiffs' electronic devices, without such reasonable suspicion, violated the Fourth Amendment.

Id. 47–48. The court denied Plaintiffs' request for expungement, *id.* 44–47, and ordered further briefing on injunctive relief. *Id.* 48–49; Order, D. Ct. Dkt. 110. The parties submitted a Joint Statement that the district court should enter declaratory relief consistent with the court's opinion and injunctive relief as to Plaintiffs. App. 356–59.

On November 21, 2019, the district court entered judgment, granting Plaintiffs declaratory relief consistent with its November 12 order.[3] Addendum 50–51. The court further granted injunctive relief barring Defendants from searching or seizing any of the Plaintiffs' electronic devices at the border "unless Defendants have reasonable suspicion that the device contains contraband." *Id.* 51. The injunction further provided that if Defendants do search a Plaintiff's device at the border based on reasonable suspicion that the device contains contraband,

[3] This declaratory judgment holds that Defendants' policies themselves are unconstitutional, so contrary to Defendants' assertion, the issues on appeal are not limited to whether those policies are unconstitutional "as applied to plaintiffs." Defs.' Br. 1, 9.

Defendants must not seize the device "longer than a reasonable period that allows for an investigatory search for that contraband." *Id.*

SUMMARY OF ARGUMENT

I. Although the district court correctly held that Defendants' policies permitting suspicionless border device searches violate the Fourth Amendment, the Fourth Amendment requires a warrant supported by probable cause.

A. Travelers have extraordinary privacy interests in the vast quantities of personal data their electronic devices contain. The Supreme Court has recognized the enormity of the privacy interests in modern electronic devices. *See Riley*, 573 U.S. at 394. Quantitatively and qualitatively, searches of electronic devices reveal far more personal information than other searches at the border, or even searches of places such as homes.

B. The Fourth Amendment requires a warrant for both basic and advanced device searches at the border. Border searches of electronic devices are untethered from the underlying rationales for the border-search exception: customs and immigration enforcement—that is, preventing the entry of inadmissible goods and persons.

C. In the alternative, this Court should affirm the district court's ruling and hold that the Fourth Amendment requires at least reasonable suspicion that an electronic device contains digital contraband for all device searches at the border. Searches of electronic devices are extraordinarily invasive and thus are unlike the kinds of routine border searches permissible without individualized suspicion.

II. Warrantless, suspicionless device searches violate the First Amendment. Such searches burden expressive and associational rights, and Defendants cannot demonstrate a compelling interest in such searches, nor a substantial relation between their interests and the personal data travelers must disclose.

III. Defendants' long-term device seizures violate the Fourth Amendment because they are conducted absent probable cause (or at least reasonable suspicion), and they lack effective limits on duration.

IV. Plaintiffs are entitled to the remedy of expungement, as Defendants continue to retain information that was acquired by unconstitutional means.

V. The district court properly determined that Plaintiffs have injunctive standing. Plaintiffs face a substantial risk that they will be subjected to future border device searches; Defendants' policies increase the risk of these future searches; and several Plaintiffs have standing to seek expungement.

STANDARD OF REVIEW

On appellate review of summary judgment, legal conclusions are reviewed *de novo*. *United Paperworkers Int'l Union Local 14, AFL-CIO-CLC v. Int'l Paper Co.*, 64 F.3d 28, 32 (1st Cir. 1995). Where the parties agree that there are no material facts at issue for trial, *see* Defs.' Br. 13 n.10, the district court's factual inferences should be set aside only if clearly erroneous. *United Paperworkers*, 64

F.3d at 31–32. *See also García-Ayala v. Lederle Parenterals, Inc.*, 212 F.3d 638, 643–45 (1st Cir. 2000).

ARGUMENT

I. The District Court Correctly Held that the Fourth Amendment Prohibits Suspicionless Device Searches at the Border, but the Fourth Amendment Requires a Warrant Supported by Probable Cause

The district court correctly concluded that suspicionless border searches of electronic devices are unconstitutional, and it correctly stated that *Riley*'s analysis of cell phone searches incident to arrest "carries persuasive weight in this context." Addendum 26–27. However, a proper consideration of how *Riley* applied the Fourth Amendment balancing test in the context of an analogous warrant exception leads to the conclusion that a warrant based on probable cause is required for border searches of electronic devices. *See United States v. Ramsey*, 431 U.S. 606, 621 (1977) (comparing the border-search exception to the search-incident-to-arrest exception).

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

This Court and the Supreme Court have recognized, and the record in this case shows, the enormity of the privacy interests at stake in today's electronic devices. Searches of such devices can reveal the "sum of an individual's private life," and they "bear[] 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." *See Riley*, 573 U.S. at 386, 393–94. As this Court explained in *United States v. Wurie*, "individuals today store much more personal information on their cell phones than could ever fit in a wallet, address book, [or] briefcase." 728 F.3d 1, 9 (1st Cir. 2013), *aff'd*, *Riley*, 573 U.S. 373. The personal information contained in some physical items carried in luggage does not approach the vast, diverse, and sensitive information accessible on electronic devices. *See Riley*, 573 U.S. at 400.

Riley held that electronic devices differ fundamentally—quantitatively and qualitatively—from physical containers. *Id.* at 393.

Quantitatively, with their "immense storage capacity," electronic devices can contain "millions of pages of text, thousands of pictures, or hundreds of videos." *Id.* 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."); SUMF ¶ 63.

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." *Wurie*, 728 F.3d at 8. *See also*

SUMF ¶ 64. 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 data provides—expressly or by inference—a detailed account of our political affiliations, religious beliefs and practices, sexual and romantic lives, financial status, health conditions, and family and professional associations. *Id.* at 395–96. The spectrum of information found on devices means they "not only contain[] in digital form many sensitive records previously found in the home; [they] also contain[] a broad array of private information never found in a home in any form—unless the phone is." *Id.* at 396–97. *See also* SUMF ¶¶ 64–66. Indeed, the Supreme Court in *Carpenter* required a warrant for a category of highly sensitive information—historical cell site location information—because "an individual maintains a legitimate expectation of privacy in the record of his physical movements." 138 S. Ct. at 2217. Many electronic devices contain this kind of information, and much more. SUMF ¶ 69.

Technological advancements amplify these privacy interests. The volume and types of data devices contain continue to grow, as does the ease with which CBP and ICE 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* and *Wurie*.

In *Ramsey*, the Supreme Court distinguished the search of a vessel or container from the search of a house. Since before the ratification of the Constitution, the latter required a warrant—even when conducted to enforce customs laws—while the former typically did not, because "a port of entry is not a traveler's home." 431 U.S. at 617, 618. *See also* 19 U.S.C. § 1595(a) (requiring warrant for customs searches of homes). But a search of an electronic device "would typically expose to the government far *more* than the most exhaustive search of a house." *Riley*, 573 U.S. at 396.

Further, *Riley* required a warrant to search the cell phones of arrestees despite their "diminished privacy interests," *id.* at 392, because the privacy interests implicated by cell phone searches were so significant. The same logic applies in the border search context. Although travelers also have "a reduced expectation of privacy" at the border, Addendum 17, "[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," *id.* at 27 (citing *Riley*, 573 U.S. at 393) (emphasis added). Moreover, the overwhelming majority of international travelers

are not suspected of any crime and thus have privacy interests that are at least equivalent to those of arrestees.[4]

The record here reflects these extraordinary privacy interests and the ease with which the government can invade them absent constitutional limits. The devices that Plaintiffs were carrying had enormous storage capacities, SUMF ¶¶ 121, 123, 125, 127, 129–30, 132, 134–35, 137, 140–42, 144, 146, 149, and contained highly personal information, *id.* ¶¶ 122, 129, 139, 142. They included photographs implicating their religious beliefs, attorney-client privileged communications, and journalistic work product. *Id.* Indeed, CBP and ICE recognize the sensitivity of searching such information. *Id.* ¶¶ 63–66.

Defendants can easily access this array of personal information through border searches of electronic devices. When CBP or ICE officers conduct basic searches, they can use the native search functions on the devices, including keyword search tools, to view files, images, or other information resident on the devices and accessible using their operating systems. *Id.* ¶¶ 67–71. This includes information from the internet that is cached on a traveler's device. *Id.* ¶¶ 75–76. Basic searches can even extend to metadata, such as the date and time associated

[4] The government cites *United States v. Boumelhem*, 339 F.3d 414, 423 (6th Cir. 2003), for the proposition that travelers have reduced privacy expectations because other countries may conduct border searches. Defs.' Br. 16. But whether and how another country conducts border searches has no bearing on the constitutional rules limiting U.S. officials.

with content, usage history, sender and receiver information, or location. *Id.* ¶ 69. Advanced searches can reveal everything basic searches reveal, and sometimes can also reveal deleted, password-protected, or encrypted data. *Id.* ¶¶ 72–73. Advanced searches may also entail making a copy of all data on a device. *Id.* ¶ 74.

Finally, the privacy risks posed by border searches of electronic devices are compounded by Defendants' sharing of device information with other federal agencies, as well as state, local, and foreign governments. *Id.* ¶¶ 14, 16, 24, 80. CBP does not know how long other government entities keep this information. *Id.* ¶ 15.

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

The district court correctly concluded that suspicionless border searches of electronic devices are unconstitutional, but it incorrectly concluded that the Fourth Amendment could be satisfied by reasonable suspicion rather than a warrant supported by probable case. The Supreme Court has not precluded requiring a warrant for certain border searches. The Court has contemplated that border searches may be unreasonable, for example, "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 *Ramsey*, 431 U.S. at 618 n.13). The Court has never suggested that reasonable suspicion is a *ceiling*, rather than a 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 152. In *Ramsey*, the Court left open the possibility that where border searches burden First Amendment rights, the "full panoply" of Fourth Amendment protections might apply. 431 U.S. at 623–24 & n.18.

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

As *Riley* reiterated, in determining whether to apply an existing warrant exception—in this case, the border-search 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. 573 U.S. at 385–86. The privacy interests that travelers have in the digital data their devices contain cannot be overstated. *See supra* Part I.A.

Crucially, governmental interests are weak where warrantless searches are "untether[ed]" from the purposes justifying the exception at issue. *Riley*, 573 U.S. at 386. The Court in *Riley* found only a weak nexus between warrantless searches of cell phones incident to arrest and the rationales for the search-incident-to-arrest exception—officer safety and evidence preservation—because such warrantless searches did not sufficiently advance those interests. *Id.* at 387–91. As this Court has stated, governmental interests are weak when warrantless searches in a

particular context are not "necessary" to advance the permissible purposes of the warrant exception. *Wurie*, 728 F.3d at 13. *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").

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

"[T]he ultimate touchstone of the Fourth Amendment is reasonableness." *Riley*, 573 U.S. at 381 (quotation marks omitted). Generally, reasonableness requires a warrant based on probable cause. *Id.* at 382. However, in limited circumstances, warrantless and 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 School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995); *City of Indianapolis v. Edmond*, 531 U.S. 32, 37, 48 (2000). As discussed below, the primary purpose of the border-search exception is customs enforcement: the interdiction of goods subject to duties and of other forms of physical contraband. A secondary purpose is preventing the entry of inadmissible persons.

The record conclusively shows that warrantless searches of travelers' electronic devices are not sufficiently tethered to the purposes of preventing the entry of inadmissible goods and persons. Moreover, travelers' extraordinary

privacy interests outweigh any legitimate governmental interests. 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. *Cf. Riley*, 573 U.S. at 386. Therefore, border searches of electronic devices require a warrant based on probable cause.

a. The Border-Search Exception Is Narrowly Focused on Interdicting Contraband, Not Gathering Evidence of Contraband or Other Potential Violations of Law

The Supreme Court has consistently emphasized that warrantless border searches are justified only by limited underlying rationales. As the district court correctly identified, the historically narrow scope of the border-search exception is limited to "preventing the entry of both contraband and inadmissible persons." Addendum 36. Nearly a century ago, the Court stated that an international traveler may be stopped at the border and required "to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in." *Carroll v. United States*, 267 U.S. 132, 154 (1925).

In the following decades, the Court repeatedly focused on customs enforcement, suggesting that it is the primary justification for the border-search exception. The Court has emphasized the government's interest in collection of

duties and the interdiction of contraband smuggled across the border to avoid duties or that would be harmful if brought into the country. In *Montoya de Hernandez,* citing *Carroll*, the Court stated, "[s]ince the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border . . . in order to *regulate the collection of duties* and to *prevent the introduction of contraband* into this country." 473 U.S. at 537 (emphasis added). *See also id. at* 538 n.1. This 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) (discussing the government's interest 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").

These cases have their roots in *Boyd v. United States*, 116 U.S. 616 (1886), which has been repeatedly cited for the proposition that the government's narrow border search authority is based on a long history of customs enforcement. Citing *Boyd*, *Carroll* stated that customs officers had authority pursuant to the earliest customs statutes to conduct border searches to interdict "merchandise which was subject to duty or had been introduced into the United States in any manner

contrary to law." 267 U.S. at 149–151. *See also Montoya de Hernandez*, 473 U.S. at 537 (citing *Boyd*, 116 U.S. at 623); *12 200-Foot Reels of Super 8mm. Film*, 413 U.S. at 126 (same); *Ramsey*, 431 U.S. at 616–19 (citing *Boyd* and discussing the "historical importance" of the first customs statute to the border-search exception); *Flores-Montano*, 541 U.S. at 153 (discussing how the border-search exception has its "historical pedigree" dating back to the first customs statute).[5]

Accordingly, lower courts have consistently recognized the limited justifications for the border-search exception. For example, the Ninth Circuit in *United States v. Cano* relied on the "narrow" scope of the exception, and *Boyd*'s teachings, to hold that "the purpose of the border search [exception] is to interdict contraband" and that the Fourth Amendment limits all warrantless border searches of devices (both manual and forensic) to the discovery of digital contraband. 934 F.3d 1002, 1013–14, 1018 (9th Cir. 2019).[6] *See also United States v. Molina-Isidoro*, 884 F.3d 287, 295 (5th Cir. 2018) (Costa, J., specially concurring) ("Detection of . . . contraband is the strongest historic rationale for the border-search exception."); *United States v. Aigbekaen*, 943 F.3d 713, 721 (4th Cir. 2019)

[5] The Supreme Court has also stated that the power to regulate who can come into the country "can be effectuated by routine inspections and searches of individuals or conveyances seeking to cross our borders." *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973).

[6] The Ninth Circuit used the terms "manual" and "forensic" in evaluating particular types of device searches.

(holding a warrant was required for an electronic device search that took place at the border but was not within the permissible scope of warrantless border searches); *United States v. Soto-Soto*, 598 F.2d 545, 549 (9th Cir. 1979) ("Congress and the courts have specifically narrowed the border searches to searches conducted by customs officials in enforcement of customs laws."). Likewise, in the context of determining admissibility, this Court has held that border officers' questions about drug activity that "had nothing to do with whether or not to admit [someone] into the country" were not "routine" and required *Miranda* warnings. *United States v. Molina-Gomez*, 781 F.3d 13, 24 (1st Cir. 2015).

Thus, the border-search exception does not extend to uncovering *evidence* of contraband or other violations of law. As the Court explained in *Boyd*, 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. at 623. *See also Molina-Isidoro*, 884 F.3d at 296–97 (Costa, J., specially concurring) (quoting *Boyd* and noting that "[n]o . . . 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").

The limited underlying rationales for the border-search exception reflect the Supreme Court's general rule that warrantless and suspicionless searches are reasonable under the Fourth Amendment only when justified by a non-law enforcement, non-criminal "primary purpose." *Edmond*, 531 U.S. at 37, 48. For example, the search-incident-to-arrest exception at issue in *Riley* is not justified by the general interest in investigating crime, but instead by the need to protect officer safety and prevent the destruction of evidence. 573 U.S. at 384–85. Likewise, the drug tests at issue in *Vernonia* were upheld as reasonable to protect the health and safety of minor student athletes, not to find evidence to prosecute drug crimes. 515 U.S. at 665. *See also Mich. Dept. of State Police v. Sitz*, 496 U.S. 444 (1990) (upholding sobriety checkpoints that advance the non-criminal purpose of roadway safety).

By contrast, the vehicle checkpoint in *Edmond* to uncover illegal narcotics was unconstitutional precisely because its primary purpose was to "uncover *evidence* of ordinary criminal wrongdoing." 531 U.S. at 42 (emphasis added). The Court explained 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." *Id.*

The Fourth Circuit's decision in *Aigbekaen* is instructive. The court held that a warrantless device search at the border to advance a pre-existing, domestic criminal investigation was so "attenuated from the[] historic rationales" permitting warrantless border searches that it did not fall within the border-search exception at all; the search was therefore unconstitutional and required a warrant. 943 F.3d at 721, 725 (quotation marks omitted). *Aigbekaen* emphasized the well-established principle that "[g]overnment may not invoke[] the border exception on behalf of its generalized interest in law enforcement and combatting crime." *Id.* at 721 (quoting *United States v. Kolsuz*, 890 F.3d 133, 143 (4th Cir. 2018) ("*Kolsuz II*")).

b. The Government Has No Cognizable Interest in Conducting Warrantless Device Searches at the Border to Gather Evidence for General Law Enforcement

Gathering evidence for general law enforcement—unrelated to customs and immigration enforcement—is completely untethered from the border-search exception's permissible purposes. Yet Defendants conduct warrantless searches of electronic devices to seek evidence of unlawful conduct with no nexus to the admissibility of goods and people. SUMF ¶¶ 82–83. For example, Defendants assert authority to gather evidence about a wide range of law enforcement, administrative, and regulatory matters, including financial, tax, environmental, consumer protection, or other laws. *Id.* ¶ 84. *Accord* Defs.' Br. 2–3, 43–45 (stating that border officers enforce laws relating to agriculture, intellectual property,

vehicle emissions, and food safety). Defendants also conduct warrantless searches of electronic devices for intelligence gathering. SUMF ¶ 86. They even search the devices of travelers who are not suspected of any wrongdoing to gather potential evidence about other people. *Id.* ¶¶ 89–90.

Defendants insist that their search authority is limited to "laws enforced or administered by CBP." Defs.' Br. 44. Yet the breadth of those laws is vast, as CPB and ICE claim to enforce hundreds of federal laws. SUMF ¶ 81. Indeed, Defendants state they are "responsible for enforcing criminal and civil laws and administering comprehensive regulatory schemes." Defs.' Br. 43. They also enforce "a host of other laws at the border on behalf of various federal agencies." *Id.* 44. *See also* SUMF ¶¶ 87–88. While Defendants might have broad statutory authority at the border, it does not follow that they also have broad constitutional authority to conduct warrantless device searches. As the Supreme Court stated in *Ramsey*, the 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 (emphasis added).

The government's interest in finding evidence of crime or other violations of law is no greater at the border than anywhere else. Yet CBP and ICE claim a prerogative to conduct border searches of electronic devices to advance pre-existing investigations. SUMF ¶ 91. Under these circumstances, the Fourth Circuit

in *Aigbekaen* required a warrant for a device search at the border. 943 F.3d at 725. *See also United States v. Kim*, 103 F. Supp. 3d 32, 59 (D.D.C. 2015) (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"); *Cano*, 934 F.3d at 1018 (recognizing "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"); *United States v. Vergara*, 884 F.3d 1309, 1317 (11th Cir. 2018) (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: 'protecting this Nation from entrants who may bring anything harmful into this country'") (citation omitted).

The government erroneously argues that *Boyd* is no longer relevant because *Warden v. Hayden*, 387 U.S. 294 (1967), overruled *Boyd*, and therefore *Boyd*'s distinction between *contraband* itself and *evidence* of contraband or other violations of law no longer controls. *See* Defs.' Br. 41–42. *Boyd*, in fact, is relevant to two lines of cases, one on warrant exceptions and the other on warrants, and *Hayden* only overturned the latter.

First, *Boyd* remains important to warrant exceptions. *Boyd* involved the forfeiture of 35 cases of plate glass because importers had failed to pay import taxes on them. 116 U.S. at 617. *Boyd*'s discussion of the government's customs enforcement authority guided the Supreme Court in later cases, including *Montoya de Hernandez*, which emphasized the limited purposes of the border-search exception. *See supra* Part I.B.2.a. Recent cases confirm that the Court generally conceives of warrant exceptions as being justified by limited rationales, as with the search-incident-to-arrest exception in *Riley*. 573 U.S. at 386.

Second, *Boyd* was once relevant to the scope of search warrants. To determine the value of the disputed plate glass, the judge ordered the importers to produce an invoice from previously imported cases. 116 U.S. at 618. The Supreme Court held that the order was unconstitutional because the invoice was evidence and not contraband. *Id.* at 638. This influenced subsequent search warrant cases. The Court in *Gouled v. United States* cited *Boyd* in rejecting search warrants "used as a means of gaining access to a man's house or office and papers solely for the purpose of making search to secure evidence to be used against him." *Gouled*, 255 U.S. 298, 309 (1921). *Hayden* overruled *Gouled*, holding that, in the context of search warrants, it was inappropriate to make a distinction between seizing "mere evidence" of crime and seizing items that the government had a "property" interest in: instrumentalities of crime, fruits of crime, or contraband. *Hayden*, 387 U.S. at

306–07, 310. But *Hayden* did not address (let alone collapse) the distinction between contraband and evidence vis-à-vis the border-search exception.

Hayden reasoned that "[t]he requirements of the Fourth Amendment"—i.e., probable cause, particularity, and a neutral and detached magistrate—"can secure the same protection of privacy" irrespective of the purpose of the search warrant. 387 U.S. at 306, 309. However, in the context of a *warrant exception*, these privacy protections do not exist; thus, warrant exceptions are only justified by limited, narrow purposes. *See Molina-Isidoro*, 884 F.3d at 296 n.7 (Costa, J., specially concurring) ("*Hayden* rejects the 'mere evidence' rule that had long prevented the government from using warrants to obtain evidence that was not itself the instrumentality of a crime or contraband. . . . 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."); *United States v. Stanley*, 545 F.2d 661, 666 (9th Cir. 1976) (noting *Boyd*'s discussion of the "original customs statute" and its continued relevance to "the present border search exemption"); *United States v. Roussel*, 278 F. Supp. 908, 911 (D. Mass. 1968) (citing *Boyd* and explaining that border searches "made solely in

the enforcement of Customs laws" are distinguishable from searches for "general law enforcement").[7]

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

Warrantless border searches of electronic devices are not sufficiently tethered to the core purpose of interdicting contraband. Border agents enforce customs laws by searching travelers' luggage, vehicles, and, if necessary, their persons. *See*, *e.g.*, *Flores-Montano*, 541 U.S. at 151 (inspecting vehicle gas tank); *Molina-Gomez*, 781 F.3d at 16 (questioning and patting down traveler). Border agents do not also need warrantless access to travelers' electronic devices for customs enforcement—to interdict either physical or digital contraband.

Physical Contraband. The historical 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

[7] Defendants cite *United States v. Gurr*, 471 F.3d 144, 149 (D.C. Cir. 2006), and *United States v. Fortna*, 796 F.2d 724, 738–39 (5th Cir. 1986), to argue that courts in border-search cases have collapsed the contraband/evidence distinction. Defs.' Br. 46–47. However, these cases involved documents discovered in border searches of luggage. Compared to border searches of electronic devices, luggage searches as a category are far less intrusive of privacy, and far more directly advance the interdiction of (physical) contraband that can be easily smuggled in a suitcase. That luggage searches may incidentally uncover documentary evidence does not expand the permissible justifications for border searches, and device searches as a separate category must be evaluated for whether they are sufficiently tethered to those justifications. *See Riley*, 573 U.S. at 385–86.

would be harmful if brought into the country. Warrantless device searches are untethered from this historical purpose. Just as *Riley* stated that "data on the phone can endanger no one," 573 U.S. at 387, physical contraband cannot be hidden in digital data.

Likewise, a Fifth Circuit concurring opinion stated, "[m]ost contraband, the drugs in this case being an example, cannot be stored within the data of a cell phone," and concluded that "this detection-of-contraband justification would not seem to apply to an electronic search of a cellphone or computer." *Molina-Isidoro*, 884 F.3d at 295 (Costa, J., specially concurring). *Accord Vergara*, 884 F.3d at 1317 (J. Pryor, J., dissenting) ("[T]he rationales underlying the border search exception lose force when applied to" cell phone searches because "cell phones do not contain the physical contraband that border searches traditionally have prevented from crossing the border.").

Evidence of Physical Contraband. Defendants argue that they should have unfettered access to travelers' electronic devices, as a categorical matter, to "search for *evidence* of schemes to smuggle [physical] contraband . . . as well as other evidence of border-related offenses." Defs.' Br. 43 (emphasis added). But as discussed above, *see supra* Part I.B.2.b, searching for evidence—even of customs violations—is outside the scope of the narrow purposes of the border-search exception, which include finding dutiable or prohibited goods themselves.

Judge Costa of the Fifth Circuit questioned 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." *Molina-Isidoro*, 884 F.3d at 296 (Costa, J., specially concurring). He explained that *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 potential ramifications for the application of the border-search authority to 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. at 297 (citation and quotation marks omitted). *See also United States v. Kolsuz*, 185 F. Supp. 3d 843, 858 (E.D. Va. 2016) (digital data "is merely indirect evidence of the things an individual seeks to export illegally—not the things themselves").

Digital Contraband. Although the district court aligned its rule with the core purpose of the border-search exception, *see infra* Part I.C.3, it ultimately failed to do a complete tethering analysis. Doing so compels the conclusion that the government's interest in conducting warrantless border device searches to interdict digital contraband is weak. Assuming digital contraband may be interdicted at the border, *cf. Thirty-Seven Photographs*, 402 U.S. at 376–77, this interdiction should not be facilitated by warrantless searches of electronic devices because the *Riley* factors are not met.

First, digital content that is itself unlawful is limited. "The forms of such contraband, as identified by Defendants, can include child pornography, classified

information and counterfeit media." Addendum 22. Yet 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.

Second, the government has not demonstrated that digital contraband is a "prevalent" problem at the border. *See Riley*, 573 U.S. at 389. As the district court concluded, Defendants proffered a "dearth of information of the prevalence of digital contraband entering the U.S. at the border." Addendum 22. The record shows that, in fact, child pornography is *primarily* transported into the U.S. via the internet, not ports of entry. SUMF ¶ 92. *See also* App. 110 (concluding that "[t]he vast majority of child pornography offenders today use the Internet or Internet-related technologies to access and distribute child pornography") (alterations in original and quoting U.S. Sent'g Comm'n, *Report to the Congress: Federal Child Pornography Offenses*, at 41–42 (2012)). This is in contrast to physical contraband such as drugs. *See, e.g., Flores-Montano*, 541 U.S. at 153 (discussing how drug "smugglers frequently attempt to penetrate our borders with contraband secreted in" vehicles).

Third, 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. This

is because, unlike physical contraband, digital contraband is *easily* transported across borders via the internet. SUMF ¶¶ 92, 95–97. *See also Vergara*, 884 F.3d at 1317 (J. Pryor, J., dissenting) ("[E]lectronic contraband is borderless."). Physical contraband is fundamentally different. Any drugs the government interdicts at a particular port of entry cannot be imported, though *other* drugs might already be in the country or may enter in some other way. But when the government interdicts digital contraband, *identical* data may already have entered the country and been distributed widely via the internet, or might do so at some other time. It is telling that Defendants do not know how effective warrantless device searches are at preventing the entry of digital files not already present in the United States and uncovering digital contraband in general. SUMF ¶ 98–99.

In sum, the record does not show that digital contraband is a sufficiently prevalent problem at the border or that interdicting it on travelers' devices prevents those same files from entering the country on the internet. Though 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.

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

Warrantless border searches of electronic devices are not 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 inspecting official documents such as passports and visas and questioning travelers. Border officers do not also need warrantless access to travelers' electronic devices to determine admissibility.

Defendants incorrectly state that the district court did not address admissibility. They declare that they do "not construe the district court's opinion as foreclosing reliance" on the admissibility rationale to conduct electronic device searches at the border. Defs.' Br. 40–41 n.18. In fact, the district court rejected the 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. Addendum 21–22, 36. *See also* SUMF ¶ 2.

Even with regard to a person who is not a U.S. citizen or lawful permanent resident, "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 district court found "there is no indication as to the frequency of same or the necessity of unfettered access to the trove of personal information on electronic devices for this purpose." Addendum 36. Thus, the record does not support the argument that suspicionless or warrantless access to travelers' electronic devices meaningfully prevents the entry of inadmissible foreign

nationals, or that any ability to prevent such entries would outweigh the acute privacy harms of conducting warrantless, suspicionless device searches for that purpose.

***

The record shows that the government's interests in conducting warrantless border device searches are: (1) nonexistent as to gathering evidence for general law enforcement; (2) weak as to interdicting physical and digital contraband; (3) nonexistent as to determining the admissibility of automatically admissible 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, travelers' extraordinary privacy interests 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. "[S]ome searches, even when conducted within the scope of [an] exception [to the warrant requirement], are so *intrusive* that they require additional justification, up to and including probable cause and a warrant." *Cano*, 934 F.3d at 1011.

e. A Warrant Requirement for Border Device Searches Would Not Impede Customs Enforcement

A warrant requirement would not impede Defendants' enforcement activities at the border.

First, where border officers have probable cause that a device contains digital contraband—or even evidence of physical contraband smuggling or crime—they can secure a search warrant.

Second, 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. The record shows that Defendants have experience and receive training in obtaining warrants for searches of electronic devices and in other contexts at the border. SUMF ¶¶ 103–115.

Third, getting a warrant need 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 in a reasonable time period. *See infra* Part III; SUMF ¶¶ 11, 21.

Finally, 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. Border officers would still need probable cause, but they could conduct a warrantless search of a device if they reasonably believe that doing so,

for example, would protect someone from imminent injury. *See United States v. Tibolt*, 72 F.3d 965, 969, 971 (1995).

C. The Fourth Amendment Requires at Least Reasonable Suspicion of Digital Contraband for All Electronic Device Searches at the Border

Should this Court decline to require a warrant for all electronic device searches at the border, it should affirm the district court's holding that such searches, whether basic or advanced, require reasonable suspicion that the device contains digital contraband. Addendum 47–48. Travelers' extraordinary privacy interests in their digital data render all device searches "non-routine" border searches requiring at least reasonable suspicion. The record in this case demonstrates that both basic and advanced searches, as defined in CBP's and ICE's policies, are extraordinarily invasive and should be treated the same for constitutional purposes. The district court also correctly held that 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-search exception: determining the admissibility of goods and people.

1. Electronic Device Searches Are Not Routine Border Searches

"Non-routine" border searches require at least reasonable suspicion. *See Montoya de Hernandez*, 473 U.S. at 541 (requiring reasonable suspicion for the detention of a suspected alimentary canal drug smuggler for a lengthy period); *Flores-Montano*, 541 U.S. at 152 (non-routine searches include those that are "highly intrusive" and impact the "dignity and privacy interests" of travelers). This Court held in *United States v. Braks*, 842 F.2d 509, 511–12 (1st Cir. 1988), that whether a search is "routine" is determined by reference to its "degree of invasiveness or intrusiveness," based on whether it abrogates reasonable expectations of privacy and the overall manner in which it is conducted.

As the district court recognized, electronic device searches are not "routine" border searches that may be conducted without suspicion. Addendum 30–34. They are highly intrusive searches at odds with reasonable expectations of privacy because of the extraordinary quantity and breadth of personal information they reveal. *See supra* Part I.A. Moreover, under Defendants' policies, device searches can be conducted after a traveler has left the border, with no meaningful limit on their duration or amount of information an officer may obtain. SUMF ¶¶ 11–13, 21–22.

While searches deemed "non-routine" are often intrusive searches of the person, such as body cavity or strip searches, *see* Defs.' Br. 17–18, 21, such

searches implicating dignity and autonomy interests in one's body are not the only means by which someone's reasonable expectation of privacy might be violated. Indeed, in *Braks*, 842 F.2d at 511, 512 n.12, this Court relied on *Winston v. Lee*, 470 U.S. 753, 762 (1985), which provided examples of intrusions such as eavesdropping and home searches that are not bodily intrusions but nonetheless "damage the individual's sense of personal privacy and security."[8] Device searches are more intrusive than these examples from *Winston*: they reveal "far *more* than the most exhaustive search of a house." *Riley*, 573 U.S. at 396. As the district court recognized, device searches can reveal a range of personal information that a body search could never reveal, including familial, religious, political, financial, medical, and other sensitive information. Addendum 30–34.

The searches at issue in this case bear this out: two Plaintiffs, for instance were deeply concerned about male officers seeing their photos without headscarves, which they wear in accordance with their religious beliefs. SUMF ¶¶ 122, 139. One Plaintiff saw an officer viewing communications with her lawyer. *Id.* ¶ 142.

[8] To the extent other courts have suggested that non-destructive property searches are categorically considered "routine," this Court should decline to follow them. *Cf.* Defs.' Br. 21. The Fourth and Ninth Circuits have held that forensic searches of electronic devices at the border—despite being property searches—are nonetheless "non-routine" and require individualized suspicion. *See Kolsuz II*, 890 F.3d at 137; *Cotterman*, 709 F.3d at 957.

Moreover, the privacy harms of device searches can be compounded by additional dignitary harms when officers look through information in the presence of the traveler and ask questions about the content in a potentially humiliating manner. For example, an officer took one Plaintiff's phone into another room for four hours and continually returned to ask him questions about its contents. *Id.* ¶ 130. The district court correctly concluded that the "potential level of intrusion from a search of a person's electronic devices simply has no easy comparison to non-digital searches," and thus held that such searches are "non-routine" and require reasonable suspicion. Addendum 30.[9]

2. Basic and Advanced Searches Are Both Non-Routine

The district court also correctly held that constitutional limitations on device searches at the border should apply to both basic and advanced searches as defined by the government's policies, because any distinction between these searches lacks practical significance and is therefore legally untenable. Addendum 30–39. The

[9] The district court exempted "cursory" searches from its rule. Addendum 31. Plaintiffs agree that border officers may inspect a device without any suspicion in order to "confirm[] that it is operational and that it contains data." *Id.* However, Plaintiffs disagree that border officers may do so to determine whether "a device is owned by the person carrying it." *Id.* Defendants have no legitimate interest in knowing this. For example, a traveler may reasonably be using a device that they do not own such as a device owned by their employer or relative. Even if Defendants can demonstrate some interest, an unbridled search for indicia of ownership by examining the contents of devices would be highly intrusive. *See supra* Part I.A.

court reasoned that "a basic search and an advanced search differ only in the equipment used to perform the search and certain types of data that may be accessed with that equipment, but otherwise both implicate the same privacy concerns." *Id.* 30.

The uncontested record shows that even a basic search "may reveal a wealth of personal information," including "sensitive information" such as "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." Addendum 30 (citing SUMF ¶¶ 63–71). Even without special training or equipment, 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. SUMF ¶¶ 70–71. Importantly, the warrantless cell phone searches that *Riley* deemed to be unconstitutionally invasive were manual. *See* 573 U.S. at 379–80, 400. *See also Kim*, 103 F. Supp. 3d at 55 (the reasonableness of a border device search does not "turn on the application of an undefined term like 'forensic'").[10]

[10] Even when a device is disconnected from the internet, border officers can still view information that originated on the internet and has been "cached" (i.e., copied) on the device. SUMF ¶ 75. Moreover, some CBP officers may have accessed cloud-based content, even after issuance of a 2017 memorandum barring such searches. *Id.* ¶ 76. *Riley* recognized the additional privacy harms of cloud searches. 573 U.S. at 397.

Defendants try to minimize the extraordinary invasiveness of basic searches by arguing that they are limited by "practical considerations," and that advanced searches are distinct because they enable "comprehensive data collection." Defs.' Br. 32–33, 36. But it is irrelevant whether every byte on a hard drive is collected and/or copied digitally, and advanced searches often do not entail such comprehensive data collection. *See, e.g.*, *United States v. Wanjiku*, 919 F.3d 472, 477 (7th Cir. 2019) (explaining that forensic EnCase software was used to "preview" defendant's hard drive, as opposed to "copy[ing] every bit of memory in the device"). What is relevant is that both basic and advanced searches *access the same files* that contain highly personal information about travelers—which can be contained within a single file or hundreds of gigabytes of data.

Moreover, Defendants' policies do not prevent border officers from manually reviewing (and memorializing) files on a device comprehensively. In fact, the policies place no limit on the scope of a basic search, because there is no ultimate limit on how long a device may be held for search or the amount of information an officer may obtain. SUMF ¶¶ 11–13, 21–22. Indeed, several of Plaintiffs' devices were detained for weeks or months. Addendum 32 n.6, 33.[11]

[11] Defendants argue that such delays might be attributable to password protection or encryption. Defs.' Br. 39 n.16. But even accounting for any such delays, there is no limitation in Defendants' policies on how long they can spend actually *searching* devices.

Officers could spend hours, days, or weeks going through the information on a device in great detail, viewing and recording it, without ever connecting it to external equipment and thereby converting it to an advanced search. Here, Plaintiffs endured device searches at the border lasting as long as 45 minutes, an hour, and four hours, SUMF ¶¶ 130, 135, 149, and several suffered long-term seizures lasting 12 days, 56 days, two months, and ten months. *Id.* ¶¶ 154, 160, 161, 166. Government agents can access a tremendous amount of private information during that time with a basic search.[12]

The district court correctly recognized that basic searches, as a category, "allow[] for both a general perusal and a particularized search of a traveler's personal data, images, files and even sensitive information," and thus should be done only with reasonable suspicion. Addendum 31, 35–38. It is inappropriate to consider the invasiveness of basic searches, as the government seems to suggest, on a case-by-case basis. Defs.' Br. 37–38. In *Riley*, it was enough that a manual search *could* reveal the massive amount of information on a device for the Court to impose a *categorical rule* that all cell phone searches incident to arrest require a warrant. 573 U.S. at 393–98. Here, the district court likewise looked to the

[12] Although the Ninth Circuit in *Cotterman* distinguished between "relatively simple" and "forensic" searches, it did not consider Defendants' policies on basic searches and the implications of unbounded searches pursuant to those policies. 709 F.3d at 960 & n.6.

invasiveness of basic searches as a category. Indeed, the government acknowledges that a "brightline rule" for advanced searches "may be more easily understood and applied by officers, enabling greater consistency and predictability in its application." Defs.' Br. 34 n.15. The same holds true for basic searches, which should all be subject to a requirement of at least reasonable suspicion.

3. Any Warrantless Border Searches of Electronic Devices Must Be Confined to Searches for Digital Contraband

a. The District Court's Rule Appropriately Tethers Warrantless Electronic Device Searches to the Primary Purpose of the Border-Search Exception

As discussed above, *see supra* Part I.B.2, warrantless border searches must be tethered to the non-law enforcement, non-evidence-gathering purposes justifying the border-search exception: preventing the entry of inadmissible goods and persons.

In holding that warrantless searches of electronic devices at the border must be justified by reasonable suspicion, the district court correctly concluded that such warrantless searches must also be limited to searches for digital contraband. The court examined the underlying purposes of the border-search exception (i.e. customs and immigration enforcement) and explained that this holding was "consistent with the government's interest in stopping contraband at the border" as well as a "long-standing distinction" in Supreme Court case law "between the

search for contraband, a paramount interest at the border, and the search of evidence of past or future crimes at the border, which is a general law enforcement interest not unique to the border." Addendum 36. Additionally, the district court's contraband limitation reflects the correct conclusion that warrantless border searches of electronic devices do not sufficiently advance the purpose of preventing the entry of inadmissible persons and thus are impermissible for this purpose. *See supra* Part I.B.2.d.[13]

b. A Reasonable Suspicion Requirement Would Provide Clear Guidance for Border Officers

The district court's requirement limiting device searches to those for digital contraband provides sufficient guidance to border officers. The government's contrary arguments are wrong for two reasons. *See* Defs.' Br. 45–46.

[13] Defendants erroneously construe the district court's opinion as permitting them to conduct border device searches that are suspicionless and unbounded by the digital contraband limitation when there are "national security concerns." *See* Defs.' Br. 40–41 n.18. The district court made the commonsense point that the national security carve-out in the CBP Policy, *see* Addendum 56 § 5.1.4, is applicable only "*to the extent that* [it] . . . is akin to the well-recognized 'exigent circumstances' exception to the warrant requirement." Addendum 21 n.5 (emphasis added). *Cf. Riley*, 573 U.S. at 388, 391, 402. Defendants are not free to use their own broad definition of "national security concern," *see* SUMF ¶ 9, to justify border device searches that do not comport with the district court's rule. Indeed, courts typically define exigent circumstances narrowly, most commonly when needed to protect someone from imminent injury. *See Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006); *Hegarty v. Somerset Cty.*, 53 F.3d 1367, 1374 (1st Cir. 1995).

First, Defendants argue that *Cano* was unclear about where border officers may reasonably search for digital contraband within an electronic device. Yet *Cano* provided a clear standard: officers "may not search [a device] in a manner untethered to the search for contraband." 934 F.3d at 1019. That is, border officers may only look in areas of a device where files and attachments comprising digital contraband might reasonably be. Thus, *Cano* correctly disapproved of border officers having "recorded phone numbers found in the call log . . . [and] photographed two messages," because the phone numbers and textual correspondence were not digital contraband. *Id.* By contrast, *Cano* also held that because "[c]hild pornography may be sent via text message, [] the officers acted within the scope of a permissible border search in accessing the phone's text messages" to determine whether the messages contained any attachments that were contraband. *Id.* This distinction is easily understood by border officers.

Second, Defendants misread *Cano*'s statement that border officers may not conduct searches of electronic devices "for evidence of past or future border-related crimes." *See* 934 F.3d at 1018, 1020. Defendants erroneously interpret this to mean that border officers may search an electronic device "for evidence that a person is engaged in smuggling contraband *at the moment of the border crossing* (for example, searching texts for evidence that the person is currently smuggling drugs)." Defs.' Br. 45. Defendants argue that this provides unclear guidance to

border officers because they "cannot know beforehand whether any evidence of a border-related offense stored on an electronic device will be of a past or future violation," which is impermissible to search for; or a present violation, which they claim is permissible to search for. *Id.* at 45–46. Defendants further object that this will supposedly require inquiry into officers' "subjective motivations." *Id.* at 46.

These concerns are unfounded. *Cano* did not endorse looking for digital evidence of *physical* contraband smuggling. Rather, *Cano* made clear that border officers may search an electronic device only to determine whether it presently contains digital contraband, such as child pornography. *Cano*, 934 F.3d at 1018. Under the *Cano* rule, searching for digital data that is itself not unlawful is simply impermissible—including text messages indicating that the traveler was, is, or will be smuggling physical contraband.[14]

II. Warrantless, Suspicionless Border Device Searches Violate the First Amendment

Defendants also violate the First Amendment by searching electronic devices at the border without a warrant or any suspicion. Government demands for

[14] *Cano* recognized that its rule is "in tension" with the Fourth Circuit in *Kolsuz II*, which involved the forensic search of the defendant's cell phone for additional evidence supporting the fact that he was smuggling firearms parts in his luggage. *Cano*, 934 F.3d at 1017 (citing *Kolsuz II*, 890 F.3d at 138–39). *See also Aigbekaen*, 943 F.3d at 721 (stating that the border-search exception's purposes include "disrupting efforts to export or import contraband"). For the reasons described, this Court should adopt the *Cano* limitation.

information revealing expressive and associational activities burden First Amendment rights, which can be justified only where the government has a compelling interest in the information and seeks no more information than necessary. *See, e.g.*, *Gibson v. Fla. Legis. Investigation Comm.*, 372 U.S. 539, 544, 546 (1963) (prohibiting a state legislative subpoena to the NAACP). Defendants do not satisfy this standard. Wholly apart from any protections required by the Fourth Amendment, a warrant is still the appropriate remedy to protect the First Amendment rights at stake here. *See Ramsey*, 431 U.S. at 624 n.18; *New York v. P.J. Video Inc.*, 475 U.S. 868, 875 (1986).

The First Amendment applies at the border. In *Ramsey*, the Court recognized that First Amendment-protected speech might be chilled by customs searches of incoming international mail. While the Court upheld the statutory search regime, it emphasized that postal regulations prohibited the reading of correspondence without a warrant. 431 U.S. at 623. The Court explicitly left open whether, absent this safeguard, it would require "the full panoply of Fourth Amendment requirements" in order to protect First Amendment rights. *Id.* at 624 n.18.

Defendants' border device searches implicate numerous First Amendment rights:

(1) the "freedom to engage in association for the advancement of beliefs and ideas," confidentially and without government scrutiny, *NAACP v. Alabama*, 357 U.S. 449, 460 (1958);

(2) the right to speak anonymously, *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995);

(3) the right to receive unpopular ideas, confidentially and without government scrutiny, *Lamont v. Postmaster Gen.*, 381 U.S. 301 (1965);

(4) the right to read books and watch movies privately, *Amazon.com LLC v. Lay*, 758 F. Supp. 2d 1154, 1167–69 (W.D. Wash. 2010); and

(5) the right to gather and publish newsworthy information absent government scrutiny of the identity of sources and journalistic work product, *Branzburg v. Hayes*, 408 U.S. 665, 709 (1972) (Powell, J., concurring); *Bruno & Stillman, Inc. v. Globe Newspaper Co.*, 633 F.2d 583, 595–96 (1st Cir. 1980).

The magnitude of First Amendment harm is illustrated by the quantity and quality of information that searches of electronic devices yield. *See supra* Part I.A. Defendants' policies grant border officers unfettered access to the contents of travelers' electronic devices, including expressive materials like emails, text messages, photos, and contacts. SUMF ¶ 64. Additionally, Plaintiffs' devices included highly sensitive information concerning their personal, privileged,

confidential, and anonymous communications and associations, *id.* ¶¶ 122, 139, 142, including journalistic information, *id.* ¶¶ 128–130, 133.

Defendants cannot satisfy the heightened scrutiny that must apply to such searches. Addendum 40–41. They cannot demonstrate that they have "overriding and compelling" interests in warrantless, suspicionless border searches of electronic devices, nor that there is a "substantial relation" between their interests and the data travelers are compelled to disclose. *See Gibson*, 372 U.S. at 546. In hope of finding evidence of unknown criminal activity, Defendants' untailored policies subject travelers to searches of *all* content on their devices, without even individualized suspicion for "basic" searches.

For searches that so burden First Amendment rights, only a warrant can adequately limit the government's access to information. *See, e.g.*, *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (holding that First Amendment interests should be protected by applying Fourth Amendment warrant standards with "scrupulous exactitude"); *P.J. Video*, 475 U.S. at 877–78 (holding that a warrant was an adequate constitutional safeguard for a search of expressive materials).[15]

[15] *See also* Michael Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. Natl. Sec. L. & Pol'y 247, 249–50 (2016) (the Fourth Amendment is tied to the First Amendment, the "papers" clause protects expressive and associational data, and a warrant should be "the constitutional default"); Daniel Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev. 112, 154, 159 (2007) (First Amendment procedural protections apply when

Contrary to the district court's suggestion, the First Amendment analysis is not subsumed by Plaintiffs' Fourth Amendment claim. *See* Addendum 42. Defendants assert that their policies "do not target speech or expression," and at most have an incidental burden on First Amendment rights. Mem. in Supp. of Defs.' Cross-Mot. for Summ. J. at 24, D. Ct. Dkt. 97. But their policies authorize unfettered access to expressive content on travelers' devices, which triggers First Amendment review. The First Amendment provides an independent check on government searches of expressive materials that separately triggers a warrant requirement. *Tabbaa v. Chertoff*, 509 F.3d 89, 102 n.4 (2d Cir. 2007) (the First and Fourth Amendments apply "different legal standards" to border searches); *Nieves v. Bartlett*, 139 S. Ct. 1715, 1731 (2019) (Gorsuch, J., concurring in part and dissenting in part) ("[T]he *First* Amendment operates independently of the Fourth and provides different protections.").

III. Defendants' Long-Term Device Seizures Violate the Fourth Amendment

The Fourth Amendment requires seizures to be (1) justified at their inception and (2) reasonable in scope and duration. *See United States v. Place*, 462 U.S. 696, 701, 709–10 (1983). Seizing and retaining a device after a traveler leaves the border must be based on at least the level of suspicion needed for the subsequent

---

there is a "chilling effect," and "a warrant supported by probable cause will, in most cases, suffice to satisfy the narrow tailoring requirement").

search, and must continue no longer than needed for the search. The district court addressed the latter claim, holding that any long-term seizure "must be for a reasonable period that allows for an investigatory search for contraband," Addendum 43, but did not address the former.

First, to be justified at its inception, any seizure to secure an item for a later search must be based on the level of suspicion required for the search itself. Any lesser standard would be unreasonable, because it would permit seizures even where subsequent searches are impermissible. *Place*, 462 U.S. at 701 ("Where . . . authorities have probable cause to believe that a container holds contraband or evidence of a crime, but have not secured a warrant, the Court has interpreted the [Fourth] Amendment to permit seizure of the property, pending issuance of a warrant to examine its contents. . . ."). Here, a probable cause warrant is required for searches of electronic devices at the border. *See supra* Part I.B. Accordingly, any long-term seizure of an electronic device pending issuance of a warrant to search it requires probable cause. At minimum, if this Court holds that reasonable suspicion is the standard to search, then the same level of suspicion is required to seize. *See* Addendum 42–43.

Second, the duration of all seizures must be reasonable, including at the border. *See id.* at 43 (detention of electronic devices must be limited to "a reasonable period that allows for an investigatory search for contraband");

Montoya de Hernandez, 473 U.S. at 542–43. Even a seizure justified at its inception becomes unreasonable if it continues too long. *See Place*, 462 U.S. at 708. *See also United States v. Mitchell*, 565 F.3d 1347, 1351 (11th Cir. 2009) (holding that a 21-day delay in securing a warrant for a computer search was unreasonable, because computers are indispensable in everyday life).

Additionally, courts require a higher standard when the length of a seizure increases. In *Place*, for example, the Supreme Court held that the detention of a domestic traveler's luggage for 90 minutes without probable cause violated the Fourth Amendment, even if a shorter detention for a cursory inspection would be justified upon reasonable suspicion. *Place*, 462 U.S. at 708–10. *See also Molina-Gomez*, 781 F.3d at 21 (suggesting that reasonable suspicion was required for a 22-day device retention); *United States v. Laich*, No. 08-20089, 2010 WL 259041, *4 (E.D. Mich. Jan. 20, 2010) (permanent seizure of laptop absent probable cause violated Fourth Amendment).

Defendants' policies do not satisfy these two requirements. They permit long-term seizures of devices absent probable cause (or any suspicion at all), and they lack any effective limit on duration. SUMF ¶¶ 11–12, 21. Plaintiffs' experiences are illustrative. Without probable cause, Defendants retained some Plaintiffs' devices for weeks and months. *See id.* ¶¶ 156, 160–61 (holding one of Allababidi's devices for ten months and another for two months); *id.* ¶¶ 162, 166

(holding Wright's devices for 56 days); *id.* ¶¶ 121, 152, 154 (holding Alasaads' devices for approximately 12 days).

Defendants do not dispute that duration must be reasonable. Instead, they argue only that the reasonableness of duration is flexible, and "does not impose rigid rules for the length of time." Defs.' Br. 48. Yet Plaintiffs do not seek "hard and fast time limits," *id.*, but rather contend that Defendants' policies provide no meaningful limit on duration whatsoever. The excessive seizures Plaintiffs experienced demonstrate the insufficiency of Defendants' policies.

IV. Plaintiffs Are Entitled to the Remedy of Expungement

While the district court correctly held that Plaintiffs have standing to seek expungement of information retained by Defendants from their unconstitutional searches of Plaintiffs' electronic devices, *see infra* Part V, the court erred in denying Plaintiffs the remedy of expungement, which is necessary to provide full relief. *See* Addendum 44–47.

Courts are "empowered to order the expungement of Government records where necessary to vindicate rights secured by the Constitution." *Chastain v. Kelley*, 510 F.2d 1232, 1235 (D.C. Cir. 1975). *See also Fazaga v. FBI*, 916 F.3d 1202, 1239 (9th Cir. 2019) ("We have repeatedly and consistently recognized that federal courts can order expungement of records, criminal and otherwise, to vindicate constitutional rights."); *Livingston v. U.S. Dep't of Justice*, 759 F.2d 74,

78 (D.C. Cir. 1985). This is true even when "the continued storage, against plaintiffs' wishes, of . . . [sensitive] information that was . . . taken from them by unconstitutional means does not *itself* constitute a violation of law"; because retention "is clearly an ongoing 'effect' of the . . . unconstitutional . . . [conduct,] expungement of the [information] would be an appropriate remedy for the . . . violation." *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1275 (9th Cir. 1998). *See also Powell v. Ward*, 643 F.2d 924, 933 (2d Cir. 1981) (expungement is an "appropriate remedy to compensate plaintiffs for the continued violation of their rights").

Expungement is accordingly warranted if the information was taken by unconstitutional means, *Norman-Bloodsaw*, 135 F.3d at 1275, or where, "as may be the case with information about . . . private and personal relationships, [it] is prejudicial without serving any proper purpose of the [government agency]," *Chastain*, 510 F.2d at 1236. The ongoing injury need not be "very great" to merit relief. *Livingston*, 759 F.2d at 78. Here, expungement is justified.

First, as the district court held, the searches of Plaintiffs' devices were carried out pursuant to policies that violate the Fourth Amendment. Addendum 36. The government therefore acquired the information from Plaintiffs' devices by "unconstitutional means." *Norman-Bloodsaw*, 135 F.3d at 1275. *See also Doe v. U.S. Air Force*, 812 F.2d 738, 740 (D.C. Cir. 1987) ("[I]f the searches and seizures

were unconstitutional, government possession of the information is at least the result of unlawful activity."). On this basis alone, expungement is warranted.

Second, the information obtained in the searches is "prejudicial without serving any proper purpose." *See Chastain*, 510 F.2d at 1236. Defendants have retained information from seven Plaintiffs' devices, including "observations or characterizations of the information contained" in the devices. Addendum 7. *See also* SUMF ¶ 150; D. Ct. Dkt. 94 (sealed exhibit). Yet Plaintiffs have never been accused of wrongdoing, and there is no suggestion that the information is relevant to any judicial or administrative proceeding.[16] Moreover, Defendants' policies allow border officers to use and share this information. SUMF ¶¶ 42, 77–80. As the district court stated, "such retention constitutes . . . ongoing and future harm as such information can be accessed by border agents and may be relevant as to whether agents otherwise might conduct a future border search of an electronic device." Addendum 14. *See also infra* Part V.A.3. (presenting the record evidence

[16] The district court erred in relying on cases involving the exclusionary rule to justify denial of expungement here. Addendum 44–45. In criminal cases, the exclusionary rule is not "designed to 'redress the injury' occasioned by an unconstitutional search." *Davis v. United States*, 564 U.S. 229, 236 (2011). Rather, the "rule's sole purpose . . . is to deter future Fourth Amendment violations." *Id.* at 236–37. Expungement, in contrast, is expressly remedial. *See, e.g.*, *Chastain*, 510 F.2d at 1235 (expungement is available "to vindicate rights"); *United States v. Coloian*, 480 F.3d 47, 49 n.4 (1st Cir. 2007) ("[F]ederal courts have upheld the expungement of criminal records as a remedy for arrests or prosecutions that violate federal statutes or the constitution.").

that information in Defendants' databases about past searches increases the risk of future searches).

Finally, the District Court erred in concluding that its injunction requiring reasonable suspicion for future searches provides adequate relief. Addendum 44–47. That requirement does not preclude Defendants from viewing, disseminating, or relying on the information unconstitutionally acquired and still retained; expungement is necessary to prevent Defendants from doing so.

V. Plaintiffs Have Injunctive Standing

Plaintiffs have shown the three basic standing elements: (1) "injury in fact"; (2) a "causal connection" to the defendant's conduct; and (3) a likelihood that a favorable decision will "redress[]" the injury. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992). Each Plaintiff has suffered an unlawful border search of their device, SUMF ¶¶ 120–49, and four have suffered unlawful long-term seizures, *id.* ¶¶ 152–66; Defendants' policies and practices caused these injuries, *id.* ¶¶ 6–24; and prospective relief will prevent recurrence.

For three independent reasons, Plaintiffs also have shown "a sufficient likelihood that [they] will again be wronged in a similar way." *City of Los Angeles v. Lyons*, 461 U.S. 95, 111 (1983). First, Plaintiffs face a substantial risk that border officers will search, seize, and retain their devices under Defendants' express policies and widespread practices. Plaintiffs regularly travel abroad. All

Plaintiffs have been searched; five were searched multiple times; one was searched four times; and two were searched after filing this lawsuit. Past searches increase the risk of future searches: when border officers decide whether to search a device, a factor is information about past border device searches in Defendants' databases. Second, Plaintiffs have probabilistic standing. Third, seven Plaintiffs have standing to seek expungement.

A. Plaintiffs Face Substantial Risk of Future Injury

Standing for prospective relief may rest, as here, on "a realistic risk of future exposure to the challenged policy." *Berner v. Delahanty*, 129 F.3d 20, 24 (1st Cir. 1997). Standing here is buttressed by Defendants' database feedback loop and recurring searches of multiple Plaintiffs. *See* Addendum 10.

1. Defendants' Policies and Practices

Defendants' policies authorize border officers to search, seize, and retain travelers' devices without a warrant and usually without suspicion. Many courts rest injunctive standing, as here, on express policies or systemic practices. *Berner*, 129 F.3d at 24; *Martinez v. Nat'l Univ. Coll.*, No. 18-1975, 2020 WL 1933646, **3–6 (D.P.R. Apr. 21, 2020); *Connor B. v. Patrick*, 771 F. Supp. 2d 142, 153 (D. Mass. 2011). For example, myriad police policies and practices support standing. *See, e.g.*, *Deshawn E. v. Safir*, 156 F.3d 340, 344–45 (2d Cir. 1998)

(interrogations); *Thomas v. Cty. of Los Angeles*, 978 F.2d 504, 506–07 (9th Cir. 1992) (searches and seizures).

Moreover, border device searches are rampant. CBP's data show 40,913 in fiscal year 2019. *See supra* n.2. Long-term seizures are also common. SUMF ¶ 55 (200 in fiscal year 2017). Such "frequency of alleged injuries inflicted by the practices at issue" supports standing. *Floyd v. City of New York*, 283 F.R.D. 153, 170 (S.D.N.Y. 2012). *See also Allee v. Medrano*, 416 U.S. 802, 815 (1974) (a "persistent pattern of police misconduct" supports injunctive relief).[17]

2. Plaintiffs' Exposure to Defendants' Policies and Practices

Plaintiffs regularly travel abroad with their devices and intend to continue doing so. SUMF ¶¶ 169–89. Most Plaintiffs purchased tickets or made specific travel plans. *Id.* ¶¶ 170, 172, 174, 176, 178, 182, 187, 189. *See also* Addendum 11.

When Plaintiffs travel, they will be exposed to Defendants' policies and practices. This establishes the requisite "realistic risk of future exposure to the challenged policy." *Berner*, 129 F.3d at 24. *See also Cotter v. City of Boston*, 193 F. Supp. 2d 323, 337 (D. Mass. 2002) (employees "exposed" to policy had

[17] This case is unlike *Lyons*, where the plaintiff did not allege the government "ordered or authorized" the challenged practice, and the plaintiff could have avoided future injury by obeying the law. *Lyons*, 461 U.S. at 106–07 & n.7. It is also unlike *Clapper v. Amnesty Intl.*, 568 U.S. 398 (2013), a pre-enforcement challenge to a law before it was applied to anyone.

standing), *rev'd in part on other grounds*, 323 F.3d 160 (1st Cir. 2003); *Connor B.*, 771 F. Supp. 2d at 150, 153 (children exposed to a foster agency's "systemic failures" had standing).

Each Plaintiff has suffered at least one border search of their device. SUMF ¶¶ 120–49. *See also* Addendum 6. Four have suffered long-term seizures. SUMF ¶¶ 152–66. Past injury is "evidence bearing on whether there is a real and immediate threat of repeated injury." *O'Shea v. Littleton*, 414 U.S. 488, 496 (1974).

3. Past Searches Increase the Risk of Future Searches

Plaintiffs' past searches increase their risk of future searches, because of how border officers use Defendants' databases. *See generally* SUMF ¶¶ 25–51. *See also* Addendum 9 ("The current record shows that agents have the potential to access information on a traveler's past searches and that such information may be used to inform decisions on future searches."); *id.* 12–13. Specifically:

- When a border officer searches a traveler's device, they can store what they find in three databases: CBP's Automated Targeting System (ATS), SUMF ¶¶ 40–41; CBP's TECS, *id.* ¶ 33; and ICE's Investigative Case Management, *id.* ¶ 50.
- With information from these device searches, ATS can "flag" a traveler. *Id.* ¶ 43. Likewise, CBP can place a TECS "lookout" for a traveler. *Id.*

¶ 27. So can other agencies, which have access to information from these device searches. *Id.* ¶¶ 14, 24, 27.

- When the traveler next crosses the border, if they have an ATS flag, *id.* ¶ 39, or a TECS lookout, *id.* ¶ 30, the CBP officer at primary inspection can refer them for secondary inspection.
- There, information about prior device searches is used in deciding whether to conduct a new device search. *Id.* ¶¶ 5, 31, 49, 51.

4. Five Plaintiffs Suffered Multiple Device Searches

Border officers searched the devices of five Plaintiffs more than once. SUMF ¶¶ 120–25, 128–30, 133–42. *See also* Addendum 6. Merchant was searched four times, three after this lawsuit was filed. SUMF ¶¶ 136–42. Allababidi was also searched after filing this suit. App. 352 (SUMF ¶ 125.1). As the district court explained: "That such search of electronic devices continues for Plaintiffs, even in the midst of their ongoing legal challenges to same, serves as further, undisputed indication of the sufficient likelihood that, unremedied, such alleged harm will continue in the future." Addendum 11. Standing is buttressed by multiple injuries to several plaintiffs. *See, e.g.*, *Creedle v. Miami-Dade Cty.*, 349 F. Supp. 3d 1276, 1289 (S.D. Fla. 2018); *Stinson v. City of New York*, 282 F.R.D. 360, 382 (S.D.N.Y. 2012); *Smith v. City of Chicago*, 143 F. Supp. 3d 741, 752 (N.D. Ill. 2015); *Aguilar v. ICE*, 811 F. Supp. 2d 803, 827 (S.D.N.Y. 2011).

B. Probabilistic Standing

Defendants' policies substantially increase the risk that border officers will subject Plaintiffs to unlawful searches and long-term seizure of their devices. "[P]robabilistic harms are legally cognizable." *Maine People's All. v. Mallinckrodt, Inc.*, 471 F.3d 277, 282, 283, 285 (1st Cir. 2006). This is an independent basis of standing: "threatened harm in the form of an increased risk of future injury may serve as injury-in-fact for Article III standing." *Baur v. Veneman*, 325 F.3d 625, 633 (2d Cir. 2003).

Plaintiffs' probabilistic injury is amplified by the severity of harm: First and Fourth Amendment violations. "The more drastic the injury that government action makes more likely, the lesser the increment in probability necessary to establish standing." *Mountain States Legal Found. v. Glickman*, 92 F.3d 1228, 1234 (D.C. Cir. 1996).

Defendants state that in fiscal year 2017, border officers searched the devices of approximately 0.007% of arriving travelers. Defs.' Br. 6. This risk (about one in 13,000) supports probabilistic standing. "[E]ven a small probability of injury is sufficient to create a case or controversy." *Massachusetts v. EPA*, 549 U.S. 497, 525 n.23 (2007). For example, plaintiffs had standing to challenge an emissions policy that created a one in 200,000 risk of skin cancer, *NRDC v. EPA*, 464 F.3d 1, 7 (D.C. Cir. 2006), and a drilling policy that created a one in 10,000

risk of an oil well fire, *Sierra Club v. Mainella*, 459 F. Supp. 2d 76, 93 (D.D.C. 2006).

Plaintiffs' actual risk is far higher than Defendants' figure. First, CBP officers do not document every device search, SUMF ¶¶ 59–62, and ICE officers do not document any basic device searches, *id.* ¶¶ 56–57. Thus, Defendants' figure is "underinclusive." Addendum 12. Second, Defendants' database feedback loop places Plaintiffs at greater risk than other travelers. *See supra* Part V.A.3; Addendum 12–13. Third, the rate of border device searches is growing quickly. CBP's jumped eight-fold between fiscal years 2012 and 2019. SUMF ¶ 52; *supra* n.2. Fourth, "lifetime risk" (not "annualized" risk) is the "more appropriate" metric. *NRDC*, 464 F.3d at 7.

C. Standing to Seek Expungement

Defendants' record systems contain information collected by border officers during searches of the devices of seven Plaintiffs. SUMF ¶ 150. *See also* Addendum 7, 14. Plaintiffs seek expungement to cure this ongoing injury from past constitutional violations.

Numerous courts have held that when law enforcement officials improperly collect information about a person, its continued retention is an ongoing injury, and that person has standing to seek its expungement. *Tabbaa*, 509 F.3d at 96 & n.2; *Hedgepeth v. WMATA*, 386 F.3d 1148, 1152 (D.C. Cir. 2004); *Paton v. LaPrade*,

524 F.2d 862, 868 (3d Cir. 1975); *Janfeshan v. CBP*, No. 16-CV-6915, 2017 WL 3972461, **4–7 (E.D.N.Y. Aug. 21, 2017); *Fox v. Dist. of Columbia*, 851 F. Supp. 2d 20, 29 (D.D.C. 2012). *Accord* Addendum 14.

CONCLUSION

Plaintiffs respectfully request that this Court hold that the First and Fourth Amendments require border officers to obtain a warrant before conducting a basic or advanced search of a traveler's device, or at least have reasonable suspicion that the device contains digital contraband. This Court should also hold that the Fourth Amendment requires border officers to have probable cause to seize and retain a traveler's device, or at least reasonable suspicion that it contains digital contraband, and that long-term seizures cannot last longer than reasonably necessary to effectuate a search. Finally, this Court should order declaratory relief that Defendants' policies and practices are unconstitutional, an injunction preventing Defendants from violating Plaintiffs' constitutional rights, and expungement of information gathered during searches of Plaintiffs' devices.

July 31, 2020

Respectfully submitted,

Adam Schwartz
Sophia Cope
Saira Hussain
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

/s/Esha Bhandari
Esha Bhandari
Hugh Handeyside
Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street,

Matthew R. Segal
BBO #654489
Jessie J. Rossman
BBO #670685
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MASSACHUSETTS,

(415) 436-9333 (phone)
(415) 436-9993 (fax)
adam@eff.org
sophia@eff.org
saira@eff.org

18th Floor
New York, NY 10004
(212) 549-2500 (phone)
(212) 549-2583 (fax)
ebhandari@aclu.org
hhandeyside@aclu.org
nwessler@aclu.org

INC.
211 Congress Street
Boston, MA 02110
(617) 482-3170 (phone)
(617) 451-0009 (fax)
msegal@aclum.org
jrossman@aclum.org

Counsel for Plaintiffs-Appellees/Cross-Appellants

CERTIFICATE OF COMPLIANCE

I herby certify that this brief complies with the type-volume limit of Fed. R. App. P. 28.1(e)(2)(B)(i) because it contains 15,291 words, exclusive of those 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.

/s/Esha Bhandari
Esha Bhandari

Counsel for Plaintiffs-Appellees/Cross-Appellants

CERTIFICATE OF SERVICE

I hereby certify that on July 31, 2020, I electronically filed the foregoing Plaintiffs-Appellees'/Cross-Appellants' Principal and Response Brief with the Clerk of the Court for the United States Court of Appeals for the First 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/Esha Bhandari
Esha Bhandari

Counsel for Plaintiffs-Appellees/Cross-Appellants