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 a/k/a 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, Chief Operating Officer and Senior Official Performing the Duties of the Commissioner of U.S. Customs and Border Protection, in his official capacity; TONY H. PHAM, Senior Official Performing the Duties of 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' REPLY 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 ii
INTRODUCTION 1
ARGUMENT 3
I. The Fourth Amendment Requires a Warrant for Electronic Device Searches at the Border, or at a Minimum Reasonable Suspicion of Digital Contraband 3
A. The Record Shows There Should Be No Legal Distinction Between Basic and Advanced Searches Under Either a Warrant or Reasonable Suspicion Standard 6
B. The Fourth Amendment Requires a Warrant for Basic and Advanced Device Searches 10
1. Travelers' Privacy Interests in Electronic Devices Are Immense 10
2. Defendants' Asserted Interests in Warrantless Border Searches of Electronic Devices Are Weak or Nonexistent 11
C. At a Minimum, the Fourth Amendment Requires Reasonable Suspicion of Digital Contraband for Basic and Advanced Device Searches 15
1. Border Device Searches Based on Reasonable Suspicion Must Be Limited to Digital Contraband 16
2. Defendants' Policies Do Not Comport with a Reasonable Suspicion Requirement for Basic or Advanced Searches 18
II. Warrantless, Suspicionless Border Device Searches Violate the First Amendment 20
III. Defendants' Policies on Long-Term Device Seizures Violate the Fourth Amendment 23
IV. Plaintiffs Are Entitled to the Remedy of Expungement 25
CONCLUSION 28
CERTIFICATE OF COMPLIANCE 30
CERTIFICATE OF SERVICE 30

TABLE OF AUTHORITIES

Cases

Arizona v. Gant,
556 U.S. 332 (2009) 5, 15

Bell v. Wolfish,
441 U.S. 520 (1979) 11

Boyd v. United States,
116 U.S. 616 (1886) 5

Carpenter v. United States,
138 S. Ct. 2206 (2018) 11

Carter v. District of Columbia,
795 F.2d 116 (D.C. Cir. 1986) 26

Chastain v. Kelley,
510 F.2d 1232 (D.C. Cir. 1975) 26

City of Indianapolis v. Edmond,
531 U.S. 32 (2000) 4, 16

Fazaga v. FBI,
965 F.3d 1015 (9th Cir. 2020) 26

Illinois v. McArthur,
531 U.S. 326 (2001) 23

Kyllo v. United States,
533 U.S. 27 (2001) 1

Norman-Bloodsaw v. Lawrence Berkeley Lab.,
135 F.3d 1260 (9th Cir. 1998) 25

Riley v. California,
573 U.S. 373 (2014) ..... passim

Terry v. Ohio,
392 U.S. 1 (1968) 15, 18

United States v. Aigbekaen,
943 F.3d 713 (4th Cir. 2019) 10, 12

United States v. Arnold,
533 F.3d 1003 (9th Cir. 2008) 21, 22

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

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013) 6

United States v. Ickes,
393 F.3d 501 (4th Cir. 2005) 21, 22

United States v. Leon,
468 U.S. 897 (1984) 26

United States v. Mitchell,
565 F.3d 1347 (11th Cir. 2009) 24

United States v. Molina-Gomez,
781 F.3d 13 (1st Cir. 2015) 13

United States v. Molina-Isidoro,
884 F.3d 287 (5th Cir. 2018) 12

United States v. Montoya de Hernandez,
473 U.S. 531 (1985) 4

United States v. Place,
462 U.S. 696 (1983) 23

United States v. Pratt,
915 F.3d 266 (4th Cir. 2019) 24

United States v. Ramsey,
431 U.S. 606 (1977) 12, 22

United States v. Thirty-Seven Photographs,
402 U.S. 363 (1971) 12

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

Warden v. Hayden,
387 U.S. 294 (1967) 5

Other Authorities

Dept. of Homeland Sec., Office of the Inspector General,
Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot (Sept. 21, 2020).....27

INTRODUCTION

Defendants attempt to minimize the invasiveness of border searches of electronic devices and argue that they conduct such searches only for narrow purposes. Their arguments are incorrect for two key reasons.

First, Defendants suggest a constitutionally significant distinction between "basic" and "advanced" searches that does not, in fact, exist. There is nothing basic about the privacy invasion of "basic" searches, and this Court should hold that both searches require a warrant. Defendants acknowledge that Fourth Amendment cases account for "significant advancements in technology that reveal to the Government information beyond what could otherwise be observed by conventional methods." Defs.' Reply 2. Yet they overlook that travelers' electronic devices themselves—not the methods used to search them—reflect a technological advancement requiring the "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *See Kyllo v. United States*, 533 U.S. 27, 34 (2001). Because of the breadth, diversity, and sensitivity of information contained on electronic devices, any search of them at the border, whether "basic" or "advanced," is an extraordinary invasion of privacy that reveals deeply personal information not only about the travelers themselves, but also about their families, friends, and colleagues. For Fourth Amendment purposes, there is no distinction between "basic" and "advanced" searches.

Second, Defendants disregard the record in this case. Ignoring the undisputed facts and extensive record below, they rely on hypotheticals and fact scenarios from other cases. But this is an appeal of a summary judgment ruling on a full record. And "[o]n this record," the district court was "unable to discern a meaningful difference between the two classes of searches"—basic and advanced—"in terms of the privacy interests implicated." Addendum 34. Nor does the record support Defendants' assertion that officers conduct device searches only for offenses that have some nexus to the border. See Defs.' Reply 32–33. The undisputed facts, including Defendants' own testimony, instead show that Defendants authorize border officers to conduct warrantless and usually suspicionless device searches at the request of domestic law enforcement agencies, to enforce a host of interior-focused laws (including tax, consumer protection, and environmental laws), and to gather intelligence on individuals other than those at the border. SUMF ¶¶ 83–91.[1]

The undisputed evidence that is actually in the record, together with the district court's well-reasoned determinations, demonstrate that the Fourth Amendment and the First Amendment require a warrant for border searches of electronic devices. But should this Court decline a warrant standard, at a minimum,

[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.

it should uphold the district court's conclusion that the Fourth Amendment requires reasonable suspicion that a traveler's device contains digital contraband for both basic and advanced device searches at the border. This Court should also hold that the Fourth Amendment limits the long-term seizure of devices: border officers must have the same level of suspicion for a long-term seizure that is required to later search it; and the duration of seizure must be limited. Lastly, this Court should grant Plaintiffs the remedy of expungement of unlawfully obtained information.

ARGUMENT

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

Defendants argue that Plaintiffs seek "a unique rule for electronic devices," Defs.' Reply 8, but Plaintiffs merely contend that the *normal* rule—that warrantless searches violate the Fourth Amendment—should not be supplanted when the government searches sensitive electronic devices at the border. Categorical exceptions to the warrant requirement depend on a "balancing of interests." *See Riley v. California*, 573 U.S. 373, 385–86 (2014). Application of a warrant exception is justifiable only if doing so is "necessary" to advance, *see United States v. Wurie*, 728 F.3d 1, 13 (1st Cir. 2013), or sufficiently tethered to, *see Riley*, 573 U.S. at 386, the limited, non-general law enforcement purposes

justifying the exception, *see City of Indianapolis v. Edmond*, 531 U.S. 32, 37, 48 (2000). Here, the record and the law demonstrate that the balance tips strongly in favor of requiring the government to get a warrant before conducting border searches of electronic devices, or, at a minimum, requiring that it conduct warrantless searches only when it has reasonable suspicion that a device contains digital contraband.

First, contrary to the government's suppositions, the record below establishes that *all* border searches of electronic searches, including those the government calls "basic," deeply threaten individual privacy. *See infra* Part I.A. Second, those privacy interests tip the *Riley* balancing test in favor of a warrant requirement because any countervailing government interests are exceedingly weak and insufficiently "tethered" to the border-search exception's core purpose: to find *dutiable or prohibited goods themselves in the items to be searched*. *See infra* Part I.B; *see also* Pls.' Principal and Response Br. ("Pls.' Br.") Part I.B.2.a.[2] Indeed, just as the Supreme Court has held that the normal warrant requirement applies to device searches of people arrested—rather than the exception for

---

[2] Plaintiffs do not contend that a search for illegal drugs falls outside the "customs" purpose underlying the border-search exception. Defs.' Reply 35 n.10. "Customs" relates to finding (physical) dutiable goods smuggled to avoid paying import taxes, and goods that are prohibited from being imported into the country, like illegal drugs, both of which are contraband. *See*, *e.g.*, *United States v. Montoya de Hernandez,* 473 U.S. 531, 537 (1985).

searches incident to arrest—it follows that the normal warrant requirement applies to device searches of travelers who are (overwhelmingly) not even suspected of any crime. *See Riley*, 573 U.S. at 391. Third, if this Court permits some warrantless searches of electronic devices, the logic of *Riley* would still mandate that they be supported by reasonable suspicion *and* limited to searching for digital contraband, as the border-search exception contemplates. *See infra* Part I.C. After all, when the government conducts a search without a warrant, and thus without its attendant findings of probable cause and particularity by a neutral and detached magistrate, the search must be strictly tethered to its purported justification. *Compare Warden v. Hayden*, 387 U.S. 294, 306–07, 309–10 (1967) (collapsing the evidence/contraband distinction for search warrants given their privacy safeguards), *with Arizona v. Gant*, 556 U.S. 332, 335 (2009) (refusing to extend the search-incident-to-arrest exception to a warrantless search of the passenger compartment of a vehicle because the search was untethered from the underlying purposes of the exception).[3]

---

[3] Nothing in *Hayden* expands the limited justifications for the border-search exception to the warrant requirement, as consistently delineated in *Boyd v. United States*, 116 U.S. 616 (1886), and subsequent cases. *See* Pls.' Br. 32–35; Amicus Br. of Constitutional Accountability Ctr. 22–26. Additionally, it is irrelevant that *Hayden* held that the search of the house where the clothing in question was found was valid pursuant to exigent circumstances. Defs.' Reply 23. Exigency is a case-by-case exception that still requires probable cause. A warrant is the default rule for the search of a home, and *Hayden* made clear that was the context at issue. *See*

A. The Record Shows There Should Be No Legal Distinction Between Basic and Advanced Searches Under Either a Warrant or Reasonable Suspicion Standard

Fourth Amendment doctrine supplies no basis to distinguish between "basic" and "advanced" device searches. Relying on detailed and undisputed facts, the district court correctly concluded that basic and advanced searches "implicate the same privacy concerns." Addendum 30. Defendants' characterizations of basic searches—as a category—as "quick," "cursory," "unintrusive," and "relatively simple," Defs.' Reply 9 (quoting *United States v. Cotterman*, 709 F.3d 952, 960 & n.6 (9th Cir. 2013) (en banc)), cannot be squared with the record. These descriptions were taken from the *Cotterman* court's discussion of a few specific manual searches rather than from the record in this case. Rather, the record shows that there is nothing basic about what Defendants' call "basic" searches; in fact, they are extraordinarily invasive. This is because 1) basic searches can deeply invade privacy, 2) Defendants' policies grant virtually unbounded discretion in how extensively to search, and 3) Plaintiffs themselves experienced highly intrusive basic searches.

First, the district court determined that basic searches are highly invasive. Basic searches provide access to the same types of data physically resident on a

---

387 U.S. at 309–10. By contrast, neither a warrant nor probable cause is the default rule when the categorical border-search exception applies.

device as advanced searches, including "prescription information, information about employment, travel history and browsing history," Addendum 30, as well as attorney-client privileged information (as demonstrated by an officer's search of a Plaintiff's device) and private photographs of travelers or their family members, *id.* 33. The district court also recognized that built-in tools enable efficient searches for specific content on phones and laptops. *Id*. 30–31. Finally, it observed that the rule in *Riley* was triggered by the amount and nature of information that officers could see—the "unfettered access to thousands of pictures, location data and browsing history," *id*. 34—rather than by the method of search, as Defendants argue, Defs.' Reply 13, 19. Indeed, any difference in *method* of search will become even more meaningless with the passage of time, "as a device's native operating systems become more sophisticated and more closely mirror the capabilities of an advanced search." Addendum 34.

Defendants argue that basic searches should be treated differently than advanced searches because the latter can provide access to deleted and encrypted data. *See* Defs.' Reply 11. But not all advanced searches enable access to such data. SUMF ¶ 73. Moreover, possible access via an advanced search to extra information in the form of deleted or encrypted data does not diminish the invasiveness of basic searches: no record evidence suggests that the nature of deleted information on devices is materially different than data viewable via a

basic search. The district court correctly understood *Riley* as concerned with the *potential* breadth of information an officer could glean from searching a phone—not whether every search *in fact* encompasses every possible piece of information on a device. Addendum 30–34.

Second, Defendants argue incorrectly that officers are limited in the time they might spend on basic searches because of the pressure of processing travelers at the border. Defs.' Reply 15–16. The record in this case, as well as Defendants' policies, demonstrate the opposite. Border officers refer travelers to secondary inspection for searches of their devices, where travelers may be held for periods of time far exceeding a normal border inspection. SUMF ¶¶ 130, 135 (searches of two Plaintiffs' devices lasted four hours and one hour); Addendum 32, 33, 38. Should an officer decide more time is required to complete a basic search, Defendants' policies allow officers to initiate a long-term seizure of the device without any ultimate limit on when it must be returned—obviating any time pressure whatsoever. *See* SUMF ¶¶ 152–54, 160–61, 166 (seizures of five Plaintiffs' devices lasted 12 days, 2 months, 56 days, and 10 months).

Third, the Plaintiffs' experiences demonstrate the invasiveness of basic searches. The officers who conducted basic searches of Plaintiffs' devices were able to record narrative descriptions of the contents of some of Plaintiffs' devices, *see* D. Ct. Dkt. 94 (sealed exhibit). Similarly, during the four-hour search of one

Plaintiff's phone, "[a]n officer periodically returned to ask [him] questions about the contents of his phone." SUMF ¶ 130. Nothing in the record supports Defendants' contention that they lack resources to conduct comprehensive basic searches. *See* Defs.' Reply 15–16.

It is no comfort to a traveler whose phone or laptop is searched without a warrant or even suspicion that a border officer might not conduct an advanced search to access deleted or encrypted material, or more efficiently record the information on the device. It is highly intrusive simply that the officer might spend hours (or days or weeks) searching through personal photographs of their children, attorney-client privileged communications, medical information, location history, browsing and search history, bank records and other financial information—all by means of manually scrutinizing this content or using built-in keyword search functions to find specific material.[4]

Nor is such a distinction between basic and advanced searches legally tenable. *Riley* made clear that even a search of a cell phone conducted by an officer on the street post-arrest is categorically privacy-invasive; the rule does not turn on

---

[4] It is also clear that during basic searches, border officers have the means to record not only descriptions of the contents of electronic devices, but also digital copies of those contents—without turning them into advanced searches by attaching the devices to any external equipment. *See United States v. Cano*, 934 F.3d 1002, 1008 (9th Cir. 2019) (officer took photograph of messages on the traveler's cell phone during a manual search).

the method or duration of search, or the data actually accessed. *See* 573 U.S. at 396. The record in this case supports the same determination here: all electronic device searches are categorically invasive.

B. The Fourth Amendment Requires a Warrant for Basic and Advanced Device Searches

Defendants argue that no court has required a warrant for searching electronic devices at the border. Defs.' Reply 5–6, 8. In fact, the Fourth Circuit requires a warrant for a border device search when the government seeks to advance a pre-existing, domestic criminal investigation. *United States v. Aigbekaen*, 943 F.3d 713, 721, 725 (4th Cir. 2019). And the Ninth Circuit requires a warrant when the government wants to access data other than digital contraband. *United States v. Cano*, 934 F.3d 1002, 1013–14, 1018 (9th Cir. 2019). Here, this Court should require a warrant for basic and advanced device searches at the border, given the strength of travelers' significant privacy interests, and the lack of sufficient tethering to the core purpose justifying the border-search exception.

1. Travelers' Privacy Interests in Electronic Devices Are Immense

The intrusiveness of both basic and advanced searches, *see* Pls.' Br. Part I.A; *supra* Part I.A, implicates significant and unprecedented privacy interests that are sufficient to trigger the Fourth Amendment's warrant requirement. Defendants erroneously argue that because cases have held that strip searches and body cavity

searches at the border often require no more than reasonable suspicion, the same must be true of searching cell phones or laptops. Defs.' Reply 7. In fact, border officers, acting under Defendants' own policies, sometimes seek warrants for body cavity searches. SUMF ¶ 108. But, in any event, the analogy between invasive physical searches and invasive electronic searches is inapt. The Supreme Court's prior holding that certain arrestees may be subject to strip or body cavity searches absent probable cause, *see Bell v. Wolfish*, 441 U.S. 520, 558–61 (1979) (pretrial detainees following contact visits), did not prevent the Court in *Riley* from holding that device searches upon arrest require a warrant, 573 U.S. at 403. Here, as in *Riley*, a warrant requirement is appropriate for device searches that can reveal the entirety of an individual's life.

Nor does it matter that other countries may conduct border searches. *Cf.* Defs.' Reply 6. A traveler's involuntary exposure of sensitive information to a third party—whether a private company or a foreign government—does not eliminate a reasonable expectation of privacy against a search by the U.S. government. *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

2. Defendants' Asserted Interests in Warrantless Border Searches of Electronic Devices Are Weak or Nonexistent

For two reasons, when weighed against the substantial privacy interests described above, governmental interests are insufficient to tip the balance in favor of warrantless searches.

First, Defendants conduct device searches for purposes far afield from the core purpose justifying the border-search exception: to find dutiable or prohibited goods themselves (i.e., contraband) *in the items to be searched. See*, *e.g.*, *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971) ("[I]nspect[ing] luggage . . . is an old practice and is intimately associated with excluding illegal articles from the country."). Defendants ignore the record evidence that their policies authorize border officers to conduct warrantless device searches for exceedingly broad purposes, including general law enforcement, that often have no connection to the border and are divorced from the core purpose of the border-search exception. *See* SUMF ¶¶ 82–84, 86–91. *See also Aigbekaen*, 943 F.3d at 721, 725.

Additionally, Defendants argue that they need warrantless access to travelers' digital data to find text messages or other digital evidence related to physical contraband smuggling (and for a host of other reasons). Defs.' Reply 21. Yet this purpose is also too attenuated from the core purpose of the border-search exception. *See*, *e.g.*, *United States v. Molina-Isidoro*, 884 F.3d 287, 296 (5th Cir. 2018) (Costa, J., specially concurring). Moreover, in *United States v. Ramsey*, 431 U.S. 606, 623 (1977), the Supreme Court acknowledged that postal regulations bar officers from reading international correspondence absent a warrant. Thus, a letter sent to the United States could discuss smuggling physical contraband (by mail or

otherwise), but officers could not read the letter without a warrant. *See* SUMF ¶¶ 106–07, 113.[5] This rule strikes the appropriate balance in advancing the government's interests—officers can obtain a warrant to read such correspondence to investigate smuggling, without chilling people from sending international mail because of the fear that government officers will read any correspondence without cause. Illogically, however, Defendants claim the same correspondence carried across the border on an electronic device could be read without a warrant or any suspicion at all. *Compare with* SUMF ¶ 114 (ICE requires a warrant to read contents of digital storage media sent through the mail).

Second, the undisputed facts show that there is insufficient tethering between warrantless searches for digital contraband and the core justification for the border-search exception, because the two *Riley* factors are not met. The record does not demonstrate that digital contraband is a "prevalent" problem at the border. *See Riley*, 573 U.S. at 389. *See also* Addendum 22. Digital content that is itself unlawful is uncommon. *See Cano*, 934 F.3d at 1021 n.13. Child pornography, the most common category of digital contraband, is *primarily* transported into the

---

[5] This Court's decision in *United States v. Molina-Gomez*, 781 F.3d 13, 15 (1st Cir. 2015), *see* Defs.' Reply 8, is inapposite because this Court did not have an opportunity to rule on the constitutionality of searching the defendant's cell phone for text messages. The motion to suppress addressed only the drugs found in the physical compartments of the defendant's electronic devices, not digital data stored on his cell phone.

United States via the internet, not on electronic devices at ports of entry. SUMF ¶ 92. Additionally, the record lacks any evidence "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. Unlike physical contraband, digital contraband is *easily* transported across borders via the internet, so bad actors have no need to carry digital contraband physically on their devices when they cross the border, and strong incentives not to. SUMF ¶¶ 92, 95–99.

Thus, a categorical rule permitting warrantless border searches of all electronic devices is unjustifiable. *See Riley*, 573 U.S. at 395 ("Allowing the police to scrutinize [cell phone] records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case."). *See also Cano*, 934 F.3d at 1011 ("[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."). Striking the appropriate Fourth Amendment balance, a warrant requirement will permit border agents to seek digital contraband—and evidence of any contraband—without enabling unfettered rummaging through travelers' voluminous personal data.

C. At a Minimum, the Fourth Amendment Requires Reasonable Suspicion of Digital Contraband for Basic and Advanced Device Searches

At the very least, all device searches—whether deemed basic or advanced—require reasonable suspicion of digital contraband. Any contrary rule would unmoor searches of electronic devices from the core purpose underlying the warrant exception for border searches, which is to find dutiable or prohibited goods themselves in the items to be searched.

This rule is categorical and easy to administer. Border officers are familiar with the reasonable suspicion standard, including its application to search for only contraband. *See* SUMF ¶¶ 106–07, 113 (requiring reasonable suspicion of contraband before international mail can be opened, and a warrant before reading correspondence). Law enforcement officers in many other warrantless search contexts also are required to have particularized, reasonable suspicion. *See*, *e.g.*, *Gant*, 556 U.S. at 346 (warrantless search of a vehicle incident to arrest permitted only where there is reasonable suspicion the vehicle contains evidence of the offense of arrest); *Terry v. Ohio*, 392 U.S. 1, 30 (1968) (warrantless pat-down search permitted only where there is reasonable suspicion the person is armed). There is no reason to treat border officers differently than all other law enforcement officers, who must adhere to reasonable suspicion standards specific to the context in which they operate.

1. Border Device Searches Based on Reasonable Suspicion Must Be Limited to Digital Contraband

Defendants nonetheless argue that warrantless border searches of electronic devices should not be limited to searches for digital contraband, because they want to additionally conduct suspicionless searches for potential *evidence* of unlawful smuggling. Defs.' Reply 20–22. But a search for potential evidence of crime is not within the core purpose for the border-search exception to the warrant requirement and cannot justify warrantless device searches. *See supra* Part I.B.2. Defendants further argue that child pornography is both contraband and evidence of crime, and thus the distinction is "illusive." Defs.' Reply 25 n.6. But the Supreme Court has made clear that although some warrant exceptions, like border searches, might result in "arrests and criminal prosecutions," that does not mean that the exceptions were "designed primarily to serve the general interest in crime control." *Edmond*, 531 U.S. at 42.[6]

Additionally, Defendants argue that they need to be able to conduct warrantless device searches for data beyond digital contraband to determine, for example, if someone has an intent to commit terrorism upon entry. Defs.' Reply

---

[6] Defendants also incorrectly assert that inspecting passports and visas constitutes a search for evidence of border-related crimes. Defs.' Reply 25 n.6. Passports and visas are required documents—things in themselves—that are necessary to enter the country. A U.S. citizen, for example, is not generally allowed to substitute their preferred "evidence" of citizenship in lieu of a passport in order to cross borders.

22. However, U.S. citizens and lawful permanent residents are always entitled to enter the country, and Defendants provide no argument for why *border officers* should be able to search U.S. persons' devices for such an intent without a warrant, given that domestic law enforcement must secure a warrant to investigate the very same potential criminal conduct. Moreover, as to all travelers, border officers have other tools at their disposal to ferret out terrorism, including the exigent circumstances exception where justified. *See*, *e.g.*, Addendum 21 n.5.

The standard Defendants urge—allowing warrantless and often suspicionless device searches for evidence of wrongdoing—lacks any meaningful limit. Defendants suggest that searches to uncover "activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern" would sufficiently restrict them to "border-related" searches. *See* Defs.' Reply 32–33 (emphasis omitted). They then cherry-pick examples from statutes that CBP is charged with enforcing. *See id*.

But the record in this case demonstrates just how broadly CBP and ICE exercise their search authority. Border officers are allowed by Defendants to search devices upon receiving information or a request from other law enforcement agencies, including the IRS, the FBI, and local police. SUMF ¶¶ 87–88. They may search devices for intelligence-gathering purposes, even when the subject of interest is someone other than the traveler. *Id.* ¶¶ 86, 89. Defendants testified that

border officers may conduct a warrantless search of a journalist's or scholar's device when they have foreign sources of interest to the U.S. government; a U.S. citizen's device for information about a suspected undocumented immigrant; and a traveler's device for evidence of their business partner's or family member's suspected wrongdoing. *Id.* ¶ 90. Rejecting virtually any limits on their enforcement purview, Defendants now ask this Court to give them unfettered authority to conduct warrantless and often suspicionless searches of devices for all of the above purposes.

This Court should not do so. The district court correctly held, as did the Ninth Circuit in *Cano,* 34 F.3d at 1013–14, that limitations on the reasonable suspicion requirement are necessary to closely tether warrantless border searches to their permissible justifications. Addendum 36–37. *See also Riley*, 573 U.S. at 386. This rule is administrable. Just as officers conducting *Terry* stops must be given training in how to conduct such searches within permissible bounds—*i.e.*, how to seek weapons only—border officers can be trained and subject to policies that ensure the device searches they conduct are for digital contraband only.

2. Defendants' Policies Do Not Comport with a Reasonable Suspicion Requirement for Basic or Advanced Searches

The district court held that both basic and advanced device searches may be conducted only where there is reasonable suspicion that an electronic device contains digital contraband. However, Defendants argue that this Court need not

address what standard the Fourth Amendment requires for warrantless searches of electronic devices in light of Defendants' policies on advanced searches. Defs.' Reply at 44–45. That is incorrect for several reasons.

First, Defendants' policies do not require reasonable suspicion for basic searches, which contravenes the district court's holding. Second, Defendants' policies do not limit device searches to digital contraband, which also contravenes the district court's holding. Third, Defendants' policies do not require reasonable suspicion for all advanced searches—the policies permit suspicionless advanced searches based on an undefined "national security concern." Addendum 5. But while Defendants suggest that a "national security concern[]" need not require reasonable suspicion, Defs.' Reply 30 n.8, the district court was clear that such an exception to its rule could be invoked only if the search satisfies the "exigent circumstances" warrant exception, Addendum 21 n.5 (citing *Riley*, 573 U.S. at 402, which similarly allowed that some device searches would not need a warrant *if* they satisfied the constitutional requirements for exigent circumstances searches).

Finally, even if Defendants' policies did meet constitutional requirements—though they manifestly do not—an individual aggrieved by a violation of the policies cannot seek redress in court. The CBP Directive explicitly states it "is an internal policy statement of [CBP] and does not create or confer any rights, privileges, or benefits on any person or party." Addendum 63. Likewise, the ICE

policy states it "is not intended to, and does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party." Addendum 73. Defendants essentially ask this Court and the public to trust the agencies not to change or derogate from their own policies (which, again, are constitutionally deficient). But, as *Riley* noted, "the Founders did not fight a revolution to gain the right to government agency protocols." 573 U.S. at 398. This Court should likewise decide the standard required for basic and advanced device searches at the border.

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

The First Amendment, like the Fourth Amendment, bars border officers from searching travelers' electronic devices without a warrant. These devices contain highly sensitive information and communications, SUMF ¶¶ 64, 122, 129–30, 133, 139, 142, implicating numerous First Amendment interests. *See* Pls.' Br. 54–55.[7] Plaintiffs do not argue here that the First Amendment requires more than the Fourth Amendment's warrant requirement. Defs.' Reply 39–42. Therefore, the

[7] *See also generally* Amicus Br. of Knight Inst. *et al.* (challenged policies burden newsgathering); Amicus Br. of Floyd Abrams *et al.* (challenged polices burden free speech). *Cf.* Amicus Br. of Constitutional Accountability Ctr. (challenged policies burden privacy of personal papers).

cases Defendants cite that reject greater protections than a warrant are inapposite.[8] Nor do Plaintiffs seek to limit searches of non-digital expressive materials, such as books. Defs.' Reply 42. Rather, Plaintiffs seek only to limit searches of electronic devices, because they are qualitatively and quantitatively more intrusive than searches of non-digital expressive materials.

Defendants rely on *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005), and *United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008), Defs.' Reply 40–41, but those cases do not deserve deference here because they preceded several key developments: Defendants' massive expansion of the frequency of border searches of devices, SUMF ¶ 52; a technological revolution in the amount of sensitive data stored in devices and built-in tools to easily retrieve such data, SUMF ¶¶ 63–76; and the Supreme Court's holding in *Riley*. Furthermore, Plaintiffs seek to protect only information in devices, not "all expressive material." *Cf. Ickes*, 393 F.3d at 506. Such protection would apply categorically to all devices, obviating any need for agents "to decide—on their feet—which expressive material" is protected. *Id.*

---

[8] *See also*, *e.g.*, Amicus Br. of Floyd Abrams *et al.* 11 ("[A]t an absolute minimum, the impact on First Amendment freedoms requires issuance of a warrant before the search of an electronic device can occur."); Amicus Br. of Knight Inst. *et al.* 15–16 ("Under the relevant First Amendment framework, suspicionless electronic device searches at the border are plainly unconstitutional. . . . [T]he government must 'get a warrant.'").

Finally, as noted above, Plaintiffs do not seek "a higher standard of probable cause" than the Fourth Amendment requires. *Id.* at 507.[9]

Additionally, Defendants ignore *Ramsey*, 431 U.S. 606, which considered the reasonableness of a warrantless search of expressive materials (international mail) in the context of regulations that "flatly prohibit[ed]" the reading of such materials without a warrant. 431 U.S. at 623. The Court left the door open to claims that less privacy-protective border search regimes (as here, where Defendants' policies explicitly allow reading the contents of devices) would "chill[]" free speech, and thus require "the full panoply of Fourth Amendment requirements," *id.* at 624 n.18—meaning a warrant. Defendants are long-accustomed to seeking warrants to read international correspondence or to open international mail not suspected of containing contraband. *Id.* at 623; SUMF ¶¶ 106–07. Requiring such time-tested constitutional protection for travelers' devices is administrable and feasible.

[9] The Court in *Arnold* explicitly relied on the reasoning in *Ickes*. 533 F.3d at 1010.

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

Defendants do not deny that the Fourth Amendment requires that device seizures be justified both at inception and in their duration. Defs.' Reply 35–38. But they incorrectly apply these principles to their policies.

Any initial seizure must be justified by at least that level of suspicion justifying the later search, but Defendants' policies do not require this because they permit seizures on no suspicion at all. *Id.* at 37–38. Outside the border context, "a seizure of personal property [is] *per se* unreasonable within the meaning of the Fourth Amendment unless it is accomplished pursuant to a judicial warrant issued upon probable cause." *United States v. Place*, 462 U.S. 696, 701 (1983). However, where there is "probable cause to believe that a container holds contraband or evidence of a crime, but [authorities] have not secured a warrant, the Court has interpreted the Amendment to permit seizure of the property, pending issuance of a warrant to examine its contents." *Id.* In other words, officers may seize an item pending later search if they have the requisite level of suspicion that would justify the search, even if they cannot immediately secure the judicial approval that the search requires. *See Riley*, 573 U.S. at 388 (with probable cause, police may seize phone incident to arrest pending application for warrant to search phone); *Illinois v. McArthur*, 531 U.S. 326 (2001) (probable cause required to seize home pending application for warrant to search home).

Plaintiffs acknowledge that border officers cannot instantaneously obtain search warrants. Instead, as in other contexts, if the search of a device requires a warrant, then upon probable cause, officers may seize the device for a reasonable amount of time required to secure the warrant. Likewise, if this Court adopts the district court's rule that reasonable suspicion is required to search, then officers must have reasonable suspicion for a longer-term seizure to search the device for digital contraband.

As to limits on the duration of seizures, Defendants' policies suffer from two main defects. First, the policies not only lack a requirement to obtain a warrant, but also a requirement that officers secure such warrant promptly. *United States v. Pratt*, 915 F.3d 266, 272 (4th Cir. 2019) (officers must "exercise diligence" in promptly seeking search warrant after seizing computer). *See also United States v. Mitchell*, 565 F.3d 1347, 1351 (11th Cir. 2009) (authorities must not unreasonably delay securing warrant for a computer search, because computers contain personal information and are indispensable in everyday life).

Second, the policies offer no guidance to officers as to what qualifies as "extenuating circumstances," SUMF ¶ 11, or "circumstances," *id.* ¶ 21, that would justify extending the seizure beyond the initial period authorized by policy (five

days for CBP and thirty days for ICE).[10] In light of the expense and inconvenience that results from being deprived of an essential communications device and the data it contains, *see* SUMF ¶¶ 153, 158, 164 (detailing Plaintiffs spending thousands of dollars to replace seized devices), more is needed to ensure reasonableness under the Fourth Amendment. Mere supervisory approval, *id.* ¶¶ 11, 21, without any further check on officers' discretion, is plainly insufficient.

IV. Plaintiffs Are Entitled to the Remedy of Expungement

Defendants concede that the district court has the equitable power to order expungement of information obtained through unconstitutional searches of Plaintiffs' devices. Defs.' Reply 42. Yet they resort to inapposite cases and misapprehend Plaintiffs' position in an attempt to justify the district court's erroneous denial of expungement. In fact, that denial constituted legal error in two respects.

First, by drawing on criminal cases deciding suppression, the court erroneously grafted a "good faith" exception into the expungement inquiry. Addendum 44–45. Yet this would often preclude expungement in the very circumstances where courts have ordered it. *See*, *e.g.*, *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1275 (9th Cir. 1998) (expungement

[10] Plaintiffs do not concede the reasonableness of these initial seizure periods.

appropriate "[e]ven if the continued storage, against plaintiffs' wishes, of intimate medical information that was allegedly taken from them by unconstitutional means does not *itself* constitute a violation of law"); *Carter v. District of Columbia*, 795 F.2d 116, 136 (D.C. Cir. 1986) (ordering expungement if the plaintiffs prevailed on Fourth Amendment claims on remand because there was "no cogent reason" to refuse such relief). Whether border officers acted "in good faith," Defs.' Reply 43–44, is not germane to expungement. Rather, in the civil context, courts have ordered expungement to vindicate rights secured by the Constitution—an inquiry that does not turn on whether the offending government personnel acted in good faith. *See generally Fazaga v. FBI*, 965 F.3d 1015, 1053–55 (9th Cir. 2020); *Chastain v. Kelley*, 510 F.2d 1232 (D.C. Cir. 1975). Quite simply, "a determination that records were obtained and retained in violation of the Constitution supports a claim for expungement relief of existing records so obtained." *Fazaga*, 965 F.3d at 1054–55.

Second, the district court erred in assuming that the costs of expungement approximate those of suppression. In criminal cases, suppression may carry a cost by allowing "some guilty defendants [to] go free." *United States v. Leon*, 468 U.S. 897, 907 (1984). No such cost exists here. Indeed, the district court failed to identify *any* harm to the government of expunging the records at issue, and Defendants offer only the unsupported and generalized assertion that expungement

would "impose costs on the Government (in destroying records)." Defs.' Reply 46. Defendants have never suggested that this unconstitutionally acquired information is necessary to aid in any investigation, nor that it relates to any allegation of wrongdoing by Plaintiffs or others. And because Defendants have already produced their notes reflecting the information gleaned from the searches of Plaintiffs' devices,[11] *see* D. Ct. Dkt. 94 (sealed exhibit), expunging these already-identified records would be virtually costless.

Considered under the proper standard, and weighed against the harm to Plaintiffs from the government's retention of their private, constitutionally protected information,[12] *see* Pls.' Br. 61–63, expungement is plainly warranted.

Finally, Defendants are wrong that the principle of constitutional avoidance somehow makes expungement improper. Defs.' Reply 44–46. Because Plaintiffs contend that *all* of Defendants' searches of Plaintiffs' devices violated the Fourth

---

[11] Notwithstanding Defendants' contrary suggestion, Defs.' Reply 44, Plaintiffs seek expungement of data copied from Plaintiffs' devices *and* border officers' narrative descriptions of the devices' contents. *See* D. Ct. Dkt. 94 (sealed exhibit).

[12] As recently demonstrated, Defendants' failure to expunge can lead to data breach and publication of travelers' personal data to the dark web. *See* Dept. of Homeland Sec., Office of the Inspector General, *Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot* (Sept. 21, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

Amendment, addressing the claim for expungement will not require any further Fourth Amendment ruling.

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 for a long-term seizure of 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. 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.

October 21, 2020

Respectfully submitted,

Adam Schwartz
Sophia Cope
Saira Hussain
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333 (phone)
(415) 436-9993 (fax)

/s/ Esha Bhandari
Esha Bhandari
Hugh Handeyside
Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street,
18th Floor
New York, NY 10004

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

adam@eff.org
sophia@eff.org
saira@eff.org

(212) 549-2500 (phone)
(212) 549-2583 (fax)
ebhandari@aclu.org
hhandeyside@aclu.org
nwessler@aclu.org

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 hereby certify that this brief complies with the type-volume limit of Fed. R. App. P. 28.1(e)(2)(C) because it contains 6,365 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 October 21, 2020, I electronically filed the foregoing Plaintiffs-Appellees'/Cross-Appellants' Reply 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