UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

GHASSAN ALASAAD et al., Plaintiffs, v. KEVIN McALEENAN, Acting Secretary of the U.S. Department of Homeland Security, in his official capacity et al., Defendants.	Civil Action No. 17-cv-11730-DJC Hon. Denise J. Casper

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT AND REPLY IN SUPPORT OF PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT

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

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Rules

Other Authorities

INTRODUCTION

The ubiquity of modern electronic devices, with their capacity to store vast quantities of highly personal information, is a new phenomenon. For most of our country's history, border officers have not had access to the types of information these devices contain, such as location history, search history, and private communications with family members, doctors, lawyers, and others. Electronic devices collect years' worth of information in one place, as well as information that never previously existed, such as metadata.

Yet Defendants seek unlimited access to all the data these devices contain, under the guise of longstanding authority to conduct certain warrantless, suspicionless searches of physical goods and people at the border—authority that would be unaffected by a ruling in Plaintiffs' favor. Border searches of digital data do not advance the same interests as border searches of physical effects. Yet Defendants claim the extraordinary power to search a wholly new category of effects amounting to "a virtual warehouse" of travelers' personal information. *See United States v. Wurie*, 728 F.3d 1, 9 (1st Cir. 2013).

The Supreme Court has rejected a "mechanical interpretation" of the Fourth Amendment, *Kyllo v. United States*, 533 U.S. 27, 35 (2001), as "technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018). This Court should deny the government's attempt to erode constitutional privacy and free speech protections, and hold that a warrant—or at least probable cause or reasonable suspicion—is required to search electronic devices at the border.

ARGUMENT

I. Warrantless, Suspicionless Searches of Electronic Devices at the Border Violate the Fourth Amendment.

In *Riley v. California*, 573 U.S. 373 (2014), the Supreme Court did not "*sub silentio* overrule centuries of practice and precedent regarding the breadth of the Government's border search authority," *cf.* Def. Mem. in. Support of Sum. Judgment, ECF No. 97 ("Def. Br."), at 2, 8–9, and Plaintiffs do not ask this Court to do so here. Rather, *Riley* demonstrates how the requisite balancing test under the Fourth Amendment must be conducted with respect to cell phone searches, and the privacy interests it identified are at least as present in this case.

A. Searches of Devices Greatly Intrude on Privacy, Even at the Border.

Defendants do not dispute that the content on electronic devices is "very sensitive." Def. Resp. to Pl. SUMF, ECF No. 98 ("Def. SUMF Resp."), at ¶¶ 63–66. Rather, they suggest people lessen their privacy interests by traveling internationally with their devices. *See* Def. Br. at 19–20. But travelers' privacy interests are not dictated by the countries they visit, and the risk that other governments may search travelers' devices does not vitiate their immense privacy interests in those devices. Even when an entity not subject to the Fourth Amendment, such as a private company or foreign government, has access to information, the Fourth Amendment still limits searches by the U.S. government. *See Carpenter*, 138 S. Ct. at 2217. Thus, the privacy interests here are at least as significant as those in *Riley*; the only potentially relevant difference is the nature of the government interests to be balanced against those privacy interests.

B. Warrantless, Suspicionless Device Searches Do Not Sufficiently Advance the Narrow Purposes of the Border Search Exception.

Defendants attempt to justify their warrantless, suspicionless searches of travelers' devices by citing the gamut of statutory and regulatory authority given to U.S. Customs and

Border Protection ("CBP") and U.S. Immigration and Customs Enforcement ("ICE"). *See* Def. Br. at 2–3. But such authorities must be exercised consistent with the Constitution, and the border search exception to the Fourth Amendment's warrant requirement is justified by two narrow purposes: determining the admissibility of goods and people. *See* Mem. and Order on Mot. to Dismiss, ECF No. 34 ("MTD Op.") at 39–40.

Defendants argue that warrantless, suspicionless electronic device searches are allowed unless they are "entirely" untethered from these justifications for the border search exception. Def. Br. at 12. But *Riley* looked at the *strength* of the nexus. The Supreme Court held that, for searches incident to arrest, there might be instances in which cell phone searches would protect officer safety and prevent evidence destruction, 573 U.S. at 387–91, but such instances were not "prevalent," and it was unclear whether "the ability to conduct a warrantless search would make much of a difference," *id*. at 389–90. *See also Wurie*, 728 F. 3d at 12 (considering whether warrantless, suspicionless cell phone searches are categorically "necessary" to serve the purposes of the search-incident-to-arrest exception).

Thus, Defendants cannot prevail by showing that warrantless, suspicionless device searches weakly (or occasionally) advance the purposes of the border search exception. As explained below, Defendants have not demonstrated that such searches sufficiently advance the narrow purposes of determining the admissibility of goods and people, so they cannot "justify dispensing with the warrant requirement across the board." *Riley*, 573 U.S. at 388.

***Digital Contraband*.** Defendants cite cases in which border officers found digital contraband on devices. Def. Br. at 13–14 & n.6. Yet Defendants do not dispute that digital data can be shared via the internet, that child pornography is primarily transferred into the country via the internet, and that digital contraband may in certain circumstances be accessible in the U.S.

via the internet. Def. SUMF Resp. at ¶¶ 92, 95–97. The government also does not dispute that it can, at most, determine whether specific digital contraband *is already* present in the United States.[1] *Id.* at ¶ 98. Moreover, Defendants do not track how many of the device searches they conduct each year uncover digital contraband. *See id*. at ¶ 99.

The interdiction of drugs or other physical contraband is fundamentally different. *Cf.* Def. Br. at 15 & n.7. Any drugs the government interdicts cannot be imported into the country, regardless of whether *other* drugs are domestically available. But when the government interdicts digital contraband, *identical* data may already have been transferred into the U.S. via the internet. *See* Def. SUMF Resp. at ¶ 97. Thus, a smattering of cases does not show that digital contraband is a sufficiently significant problem at the border or that interdicting it on travelers' devices prevents those same files from entering the country via the internet. This interest does not outweigh travelers' overwhelming privacy interests.

Evidence of Physical Contraband. Defendants also cite cases that involved discovery of digital evidence of smuggling contraband ("evidence of illegal goods") such as drugs and weapons, Def. Br. at 13 & n.6, but device searches in this context do not sufficiently advance the government's permissible interests. A search for *evidence* of customs violations is not a historical justification for the border search exception. *See Boyd v. United States*, 116 U.S. 616, 623 (1886) (distinguishing "goods liable to duties" from "seizure of a man's private books and papers" to use "as evidence against him"); *United States v. Molina-Isidoro*, 884 F.3d 287, 297 (5th Cir. 2018) (Costa, J., specially concurring) (explaining that *Boyd* made an "emphatic

[1] The government's argument that a warrant requirement for device searches would incentivize criminals to store digital contraband and evidence in those devices, Def. Br. at 18, ignores the ease with which wrongdoers already can instead store such data in the cloud and access it once they have entered the country. Thus, a warrant requirement for device searches is immaterial to whether the government can keep digital data out of the country.

distinction between the sovereign's historic interest in seizing imported contraband and its lesser interest in seizing records revealing unlawful importation"). Defendants cite *Warden v. Hayden*, 387 U.S. 294, 309–10 (1967), *see* Def. Br. at 15, but that case did not involve a border search, and the search it upheld was based on exigency, supported by probable cause, and involved clothing that was not "communicative." *Hayden*, 387 U.S. at 302–03. Nothing in *Hayden* purports to expand the purposes of the border search exception to encompass the seeking of evidence, as opposed to contraband itself. In short, a regime of warrantless, suspicionless device searches cannot be justified because it may incidentally—or intentionally—reveal such evidence.[2]

Evidence Obtained for General Law Enforcement. Defendants are even further afield from the purposes of the border search exception when they search devices for evidence that may be useful for general law enforcement. *Cf.* Exh. B, ECF No. 98-2 ("Denton Decl."), at ¶ 9 (discussing enforcement of consumer protection, tax fraud, and vehicle emissions standards laws). To be upheld, categorical exceptions to the warrant requirement require a justification separate from general law enforcement. *See Riley*, 573 U.S. at 382 ("[W]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant."); *City of Indianapolis v. Edmond*, 531 U.S. 32, 48 (2000) (the "primary purpose" of warrantless, suspicionless searches based on special needs must go "beyond the general interest in crime control"). *See also Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (same). This Court need not look at

[2] The border searches uncovering evidence in *United States v. Gurr*, 471 F.3d 144, 149 (D.C. Cir. 2006), and *United States v. Levy*, 803 F.3d 120, 124 (2d Cir. 2015), *see* Def. Br. at 15–16, involved the discovery of physical objects following searches of luggage. And the court in *United States v. Kolsuz* left open the question whether a warrant is required for border searches of electronic devices. *See* 890 F.3d 133, 137 (4th Cir. 2018).

the "underlying intent or motivation of the officers involved" in individual device searches. *See* Def. Br. at 16–17. But this Court must look at the *interests the government asserts* in favor of its program of warrantless, suspicionless device searches. *See, e.g.*, *Riley*, 573 U.S. 373 (scrutinizing the government's asserted interests in application of the search-incident-to-arrest exception to cell phones). Moreover, CBP's and ICE's collaboration with other agencies for broad law enforcement activities, *see* Def. Br. at 16–17, cannot *expand* the longstanding, limited rationales for warrantless, suspicionless border searches.

Defendants assert an interest in interdicting "criminals" (as distinct from contraband). *See* Def. Br. at 17. But U.S. citizens and lawful permanent residents are entitled to re-enter the country, *see* Def. SUMF Resp. at ¶ 2, and the government has no greater interest *at the border* in finding evidence of potentially prosecutable misconduct that occurred elsewhere.

Defendants further argue that warrants are unworkable because border officers do not have much advance information about arriving individuals. Def. Br. at 17. But they fail to explain why such notice is necessary. Police lack notice during traffic and sidewalk stops, and they must formulate the level of suspicion necessary for detention or searches based on the available information. Defendants concede that ICE agents "almost always" have reasonable suspicion before searching a device, *see* Denton Decl. at ¶ 12, showing that other border officers can do so, too. Moreover, border officers have access to the Advance Passenger Information System ("APIS"), which provides information about passengers traveling by air prior to their arrival. *See* Pl. Resp. to Def. SUMF at ¶ 14 (filed concurrently with the instant brief).

Finally, the fact that courts have not previously required a warrant for border searches is not dispositive. Defendants argue that even "non-routine" searches can require no more than reasonable suspicion. Def. Br. at 7–8. But the Supreme Court has never suggested that the

reasonable suspicion it required for the non-routine seizure and search in *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985), is a ceiling rather than a floor. *See* Pl. Mem. in Support of Sum. Judgment, ECF No. 90-1 ("Pl. MSJ Br."), at 19–20. To the contrary, the Court has explicitly considered the possibility that a border search may be constitutionally "unreasonable" because of the particularly offensive manner in which it is carried out, *see United States v. Flores-Montano*, 541 U.S. 149, 154 n.2 (2004), and that a warrant might be needed for a border search of international mail, *see United States v. Ramsey*, 431 U.S. 606, 618 n.13 (1977). Searches of electronic devices may be considered "non-routine" because they are highly intrusive of personal privacy, and nothing prevents this Court from finding that a warrant is required in this context. *See* Pl. MSJ Br. at 19–20.[3]

C. Plaintiffs' Fourth Amendment Claim Is Not Excessive in Scope.

Defendants misapprehend the nature of Plaintiffs' Fourth Amendment claim when they argue that it is overbroad. Def. Br. at 10–12. Plaintiffs do not challenge searches where "an officer merely verifies that a laptop is operational and contains data." *Id*. at 11. Instead, Plaintiffs argue that every warrantless, suspicionless search of the *digital data* on an electronic device at the border violates the Fourth Amendment. *See* Pl. MSJ Br. at 21. This includes even a "brief manual search," *cf*. Def. Br. at 11, which can access a trove of highly personal information, *see*

[3] Defendants argue that suspicionless searches of a shipping container or motor home are comparable to searches of electronic devices. *See* Def. Br. at 7 (citing *United States v. Boumelhem*, 339 F.3d 414, 417 (6th Cir. 2003), and *United States v. Cybulski*, No. 1:08-CR-8, 2009 WL 3734052, at *2 (D. Vt. Oct. 29, 2009)). But electronic device searches "typically expose to the government far *more* than the most exhaustive search of a house" because a cell phone "contains a broad array of private information never found in a home in any form." *Riley*, 573 U.S. at 396–97 (emphasis in original). Furthermore, searches of physical effects are clearly tethered to a core justification for the border search exception—keeping out contraband goods—in a way that searches of digital data are not. *See* MTD Op at 39; *Montoya de Hernandez*, 473 U.S. at 537 (purpose of warrantless border searches is "to regulate the collection of duties and to prevent the introduction of contraband").

Def. SUMF Resp. at ¶¶ 67–70. *Riley* required a warrant for manual cell phone searches, and the Court fashioned no separate rule based on the duration of a search. *See* 573 U.S. 373.[4]

Defendants also argue that Plaintiffs' Fourth Amendment claim cannot encompass all electronic devices and that Plaintiffs fail to define the scope of "electronic devices." Def. Br. at 10 & n.4. But CBP's own Directive defines an electronic device as "[a]ny device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players." Exh. F, ECF No. 98-6 (CBP 2018 Directive), at ¶ 3.2. The Fourth Amendment requires a warrant to search all of these high-volume devices.[5] However, should this Court determine that the Fourth Amendment only requires a warrant to search a narrower set of devices—for example, cell phones and computers—it can tailor the relief to the scope of the constitutional violation. *See Rosario-Torres v. Hernandez-Colon*, 889 F.2d 314, 321 (1st Cir. 1989) (the "hallmark of equity is the ability to assess all relevant facts and circumstances and tailor appropriate relief on a case by case basis").

II. This Court May Order a Probable Cause or Reasonable Suspicion Requirement.

This Court may fashion whatever remedy it deems appropriate for proven constitutional violations. *See id.* Plaintiffs seek an injunction requiring warrants based on probable cause as a

[4] Fourth Amendment facial challenges are frequently successful. *See, e.g.*, *City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2449, 2451 (2015); *Ferguson v. City of Charleston*, 532 U.S. 67, 86 (2001); *Chandler v. Miller*, 520 U.S. 305, 308–309 (1997); *Payton v. New York*, 445 U.S. 573, 574, 576 (1980); *Torres v. Puerto Rico*, 442 U.S. 465, 466, 471 (1979).

[5] *See, e.g.*, *United States v. Comprehensive Drug Testing, Inc*., 513 F.3d 1085, 1145 (9th Cir. 2008) (describing a megabyte as "the equivalent of 500 double-spaced pages of text" and a gigabyte as "the equivalent of 500,000 double-spaced pages of text"); *United States v. Green*, No. 12-CR-835, 2016 WL 3610331, at *14 (W.D.N.Y. July 6, 2016) (hard drives with a terabyte of storage "can hold approximately 1000 hours of video, 250,000 four-minute songs, 1,000,000 thick books").

cure for the claimed constitutional violations. Am. Compl., ECF No. 7 ("Compl."), at ¶¶ 169, 171. Plaintiffs also explicitly seek "such other and further relief as the Court deems proper." *Id.* at 42, ¶ K. A court may order a different remedy than the one pressed by a plaintiff where it finds a constitutional violation. *See* Fed. R. Civ. P. 54(c) (final judgment "should grant the relief to which each party is entitled, even if the party has not demanded that relief in its pleadings"); *Town of Portsmouth v. Lewis*, 813 F.3d 54, 61 (1st Cir. 2016).

Defendants incorrectly contend that Plaintiffs waived their request for an alternative remedy. Def. Br. at 21. Plaintiffs have consistently argued that, should this Court find that a warrant is not required, it should hold that electronic device searches at the border must be based on at least probable cause or reasonable suspicion. *See* Pl. Mem. in Opp. to Def. Mot. to Dismiss, ECF No. 19, at 22–24 (setting out, under a separate heading, caselaw to support Plaintiffs' request for a probable cause or reasonable suspicion requirement); Pl. MSJ Br. at 19–20 (same); Joint Statement and Proposed Discovery Schedule, ECF No. 58 ("Joint Statement"), at 2, 4–5 (seeking this alternative remedy); Compl. at ¶¶ 1, 9, 57–59, 61, 156 (objecting to "suspicionless" border searches of electronic devices or the lack of "reasonable suspicion" and "individualized suspicion"). Thus, Defendants cannot argue that Plaintiffs, by seeking an alternative remedy, have "sandbagged" them, *see United States v. Taylor*, 54 F.3d 967, 972 (1st Cir. 1995), or deprived them of "fairness, judicial economy, and practical wisdom," *Nat'l Ass'n of Soc. Workers v. Harwood*, 69 F.3d 622, 627 (1st Cir. 1995).

III. The Fourth Amendment Requires the Government to Have Probable Cause Before Confiscating an Electronic Device After a Traveler Has Left the Border.

Defendants fail to counter Plaintiffs' argument that—at its inception—a confiscation of an electronic device at the border must be based on at least the level of suspicion needed for the subsequent search in order to be constitutionally reasonable. In *United States v. Molina-Gomez*,

the First Circuit considered a 22-day detention of a laptop and gaming console for a *physical* search of the devices for drugs and concluded that reasonable suspicion supported the search. 781 F.3d 13, 19–20 (1st Cir. 2015). Thus, that case does not address the standard that applies to a confiscation of an electronic device for the purpose of searching its *data*. *Cf.* Def. Br. at 22. *Montoya de Hernandez* also does not help Defendants, *cf.* Def. Br. at 22, because there the Court held that the detention of a traveler at the border had to be justified by the requisite level of suspicion at its *inception*. *See* 473 U.S. at 541.

Plaintiffs' confiscation claim must be understood in tandem with their search claim: where the government does not have probable cause to keep an electronic device after a traveler has left the border, such a confiscation is constitutionally unreasonable, because the government does not have the probable cause to secure a warrant. *See United States v. Place*, 462 U.S. 696, 701, 709–10 (1983) (Fourth Amendment requires seizures to be justified at their inception).

Defendants do not dispute Plaintiffs' separate argument that the duration of an electronic device seizure must be reasonable; instead, they merely urge consideration of "relevant facts and circumstances" such as the availability of equipment or software. Def. Br. at 23. Notably, Defendants do not defend their policies as satisfying the reasonableness requirement. Plaintiffs do not seek an "arbitrary and inflexible time limit," *id.*, but rather contend that Defendants' policies on device confiscations, which provide for no meaningful limit on duration whatsoever, *see* Pl. MSJ Br. at 22–23, are unreasonable under the Fourth Amendment.

IV. A Regime of Warrantless, Suspicionless Searches of Electronic Devices at the U.S. Border Violates the First Amendment.

The First Amendment provides an independent check on government searches of expressive materials—including those contained in travelers' electronic devices. Thus, Defendants are wrong to suggest that Plaintiffs cannot raise a First Amendment claim in addition

to their Fourth Amendment claim, or that they are seeking an unprecedented "First Amendment exception" to the Fourth Amendment's border search exception. Def Br. at 23, 25.

In *Ramsey*, the Supreme Court separately considered whether international mail searches violated the First and Fourth Amendments. *See* 431 U.S. at 623–64. *See also New York v. P.J. Video, Inc.*, 475 U.S. 868, 873 (1986) (the "seizure of films or books on the basis of their content implicates First Amendment concerns not raised by other kinds of seizures"); *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.") (emphasis in original).[6]

Here, Defendants cannot satisfy *any* level of heightened scrutiny, including intermediate scrutiny. Per *Gibson v. Fla. Legis. Investigation Comm.*, 372 U.S. 539, 546 (1963), Defendants cannot demonstrate that they have "overriding and compelling" interests in conducting warrantless, suspicionless border searches of electronic devices, *see supra* Part I.B., or a "substantial relation" between their interests and the data travelers are compelled to disclose. *See* MTD Op. at 49 (citing *Gibson*, 372 U.S. at 546). Defendants' policies—subjecting travelers to searches of *all* content on their devices—are by definition an untailored approach.

Defendants assert that their policies "do not target speech or expression at all," and at most have an incidental burden on First Amendment rights, because their goal is to ferret out

[6] The holdings in *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005), and *United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008), *see* Def. Br. at 25, are distinguishable. Those cases rested on factual assumptions that are not applicable here. The *Ickes* court deemed it "far-fetched" that any traveler could be subjected to a laptop search given limited time and resources, 393 F.3d at 507, assuming that any such search would occur only after the discovery of physical contraband or because of a traveler's conduct, *id*. The *Arnold* court explicitly relied on the analysis in *Ickes*. *See Arnold*, 533 F.3d at 1010.

"contraband or evidence of the violation of federal laws." Def. Br. at 24. But their challenged policies grant border officers unfettered access to the content on travelers' electronic devices—which includes indisputably expressive materials such as emails, text messages, photos, and contacts. *See* Def. SUMF Resp. at ¶ 64. It is this data that is precisely the "evidence" of violations of federal law that Defendants seek. Government access to this data directly implicates a variety of First Amendment rights. *See* Pl. MSJ Br. at 23–24. *See also* MTD Op. at 51.

While the First and Fourth Amendments provide independent bases by which to evaluate the constitutionality of warrantless, suspicionless border searches of electronic devices, the appropriate *remedy* to cure violations of both Amendments is a warrant. *See Ramsey*, 431 U.S. at 624 n.18; *P.J. Video*, 475 U.S. at 875.

Additionally, Plaintiffs' First Amendment claim, like their Fourth Amendment claim, is premised on the argument that border searches of electronic devices are constitutionally problematic as a categorical matter because such searches necessarily entail the reading of content. A warrant requirement for all electronic device searches at the border would avoid any need for officers to make case-by-case decisions about whether a particular device search implicates expressive materials. *Cf.* Def. Br. at 26. *See also* MTD Op. at 50 (noting *Riley* distinguished cell phones from other categories of objects).

V. Plaintiffs Have Standing to Seek Injunctive Relief.

A. Plaintiffs Have Standing to Seek Expungement.

Plaintiffs seek to expunge information Defendants concede they retain. *See* Def. SUMF Resp. at ¶ 150. *Cf.* Def. Br. at 30 n.16.[7] Defendants' argument that Plaintiffs face no injury from this undisputed retention ignores the cases demonstrating plaintiffs' standing to seek, and the

[7] Plaintiff Wright withdraws his plea for expungement. *See* Exh. L, ECF No. 98-12 (Tsang Decl.), at ¶ 6.

courts' power to order, expungement of unlawfully collected information. Pl. MSJ Br. at 25–26. *See also Janfeshan v. CBP*, No. 16-cv-6915, 2017 WL 3972461, at **4–7 (E.D.N.Y. Aug. 21, 2017); *Fox v. District of Columbia*, 851 F. Supp. 2d 20, 29 (D.D.C. 2012). Retention of unlawfully obtained information is itself an ongoing injury, because Defendants remain free to use it against Plaintiffs, and to share it with other agencies to do the same. Pl. MSJ Br. at 26. *Cf.* Def. Br. at 29. Additionally, it can be stolen—as recently happened to a vast trove of CBP-collected images of travelers' faces and license plates. *See* Drew Harwell & Geoffrey A. Fowler, *U.S. Customs and Border Protection Says Photos of Travelers Were Taken in Data Breach*, Wash. Post, June 10, 2019.[8] *See also Paton v. La Prade*, 524 F.2d 862, 868 (1975) (retention "results in 'injuries and dangers' that are plain enough").

In Plaintiffs' cases, expungement redresses the ongoing injury. *Cf.* Def. Br. at 29, 30 & n.16. Defendants' cases are inapposite. *Id*. at 29–30. In *Kissinger v. Reporters Comm. for Freedom of the Press*, 445 U.S. 136, 147–48 (1980), and *Parole Bd. v. Scott*, 524 U.S. 357 (1998), expungement is not addressed. In *Laird v. Tatum*, 408 U.S. 1, 11 (1972), the challenged program was not applied to the plaintiff.

B. Plaintiffs Have Standing Because of the Substantial Risk of Future Injury.

All Plaintiffs face a substantial risk of future border searches and confiscations of their electronic devices because they have already been subjected, and will continue to be exposed, to Defendants' policies and practices when they travel abroad. Pl. MSJ Br. at 27–28.[9]

[8] *Available at* https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/.

[9] This Court need not address the factual predicate for past searches and confiscations of Plaintiffs' devices. *See* Joint Statement at 5. If this Court disagrees, the next step is further discovery, *id.*, not immediate resolution of privilege assertions. *Cf.* Def. Br. at 27 n.12.

Defendants assert that Plaintiffs whose devices have been searched only once face no greater risk than other travelers. Def. Br. at 27. But one past search supports standing.[10] Even if Plaintiffs faced the same odds as other travelers, injury exists "where a harm is concrete, though widely shared." *Fed. Election Comm'n v. Akins*, 524 U.S. 11, 24 (1998). *See also Lujan v. Defs. of Wildlife*, 504 U.S. 555, 572–74 (1992); MTD Op. at 23.

Moreover, the undisputed record demonstrates that past border scrutiny raises the risk of future border scrutiny. Defendants' databases maintain records of past searches, which include information from Plaintiffs' devices; officers may access such records when Plaintiffs cross the border; and officers may rely on them when deciding whether to conduct a device search. Pl. MSJ Br. at 30. Defendants concede most of the underlying facts. Def. SUMF Resp. at ¶¶ 25–26, 34–37, 44, 48–49, 150. Although Defendants assert that CBP officers at primary inspection "generally" do not have access to information about earlier device searches, Def. Br. at 5 n.1, they do not dispute that these officers *do* use the TECS database to identify "lookouts" and recent border crossings, Def. SUMF Resp. at ¶ 29, and will sometimes have information about earlier device searches. Likewise, Defendants concede that CBP officers and ICE agents in secondary inspection have access to all of this information. *Id*. at ¶¶ 34–35, 48–49.

As to Plaintiffs whose devices were searched multiple times, Defendants object that three Plaintiffs have not been searched since August 2017, and the fourth was not searched during her last five trips. Def. Br. at 28–29. Plaintiffs filed this case in September 2017, one month after a search of Plaintiff Nadia Alasaad, two months after a search of Plaintiff Kushkush, and nine months after a search of Plaintiff Dupin. Def. SUMF Resp. at ¶¶ 123, 130, 135. A rule against

[10] *See Hernandez v. Cremer*, 913 F.2d 230, 235 (5th Cir. 1990); *Ligon v. New York*, 288 F.R.D. 72, 81 n.52 (S.D.N.Y. 2013); *Floyd v. City of New York*, 283 F.R.D. 153, 169–170 (S.D.N.Y. 2012); *Ortega-Melendres v. Arpaio*, 836 F. Supp. 2d 959, 987 (D. Ariz. 2011); *Roe v. City of New York*, 151 F. Supp. 2d 495, 503 (S.D.N.Y. 2001).

standing here would incentivize the government to evade judicial oversight by leaving plaintiffs alone during the pendency of suit. *Cf. United States v. W. T. Grant Co.*, 345 U.S. 629 (1953). What is more, Plaintiff Merchant has been searched three times *after* filing suit. Def. SUMF Resp. at ¶¶ 137, 140–42, and Defendants ignore the many judicial decisions that credit multiple intrusions when finding standing for injunctive relief. Pl. MSJ Br. at 28.

Finally, Plaintiffs have an alternative basis for standing: probabilistic injury. Pl. MSJ Br. at 27–29. Plaintiffs' odds are higher than the one in 10,000 chance a traveler faced of a device search in fiscal year 2017, *see* Def. Br. at 27, because Plaintiffs are at greater risk than other travelers, as explained above, and because the overall search rate is growing each year. Pl. SUMF, ECF No. 90-2, at ¶ 52. Additionally, "lifetime risk" is a "more appropriate" metric than "risk in annualized terms." *NRDC v. EPA*, 464 F.3d 1, 7 (D.C. Cir. 2006). In any event, the unadjusted risk suffices. *Cf. id.* (1 in 200,000 risk); *Sierra Club v. Mainella*, 459 F. Supp. 2d 76, 93 (D.D.C. 2006) (1 in 10,000 risk). *See also* MTD Op. at 23. Further, the "more drastic" the threatened injury, "the lesser the increment in probability" required. *Mountain States Legal Found. v. Glickman*, 92 F.3d 1228, 1234 (D.C. Cir. 1996). Here, the threatened privacy intrusion—into all aspects of a traveler's life—is severe.[11]

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that the Court grant Plaintiffs' Motion for Summary Judgment and deny Defendants' Motion for Summary Judgment.

[11] Defendants' cases on future injury, Def. Br. at 27–28, do not suggest otherwise. In *Maine People's All. v. Mallinckrodt, Inc.*, 471 F.3d 277, 282–83, 285 (1st Cir. 2006), the court rested standing on "probabilistic harms." In *Kerin v. Titeflex Corp.*, 770 F.3d 978, 983 (1st Cir. 2014), the court rejected standing absent past injury, but held "a small probability of a great harm may be sufficient." In *Blum v. Holder*, 744 F.3d 790, 797 n.9 (1st Cir. 2014), the court rejected pre-enforcement standing where the government disavowed enforcement, mentioning probabilistic harm only in a footnote. In *Conservation L. Found. v. Pub. Serv. Co. of N.H.*, 2012 WL 4477669, at *11 (D.N.H. 2012), the plaintiff could not enjoin pollution that had ended years earlier.

Respectfully submitted: Dated: July 3, 2019

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

/s/ Esha Bhandari
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

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

*Admitted *pro hac vice*
Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I certify that on July 3, 2019, a copy of the foregoing was filed electronically via the Court's ECF system, which effects service upon counsel of record.

/s/ Esha Bhandari

Esha Bhandari