UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

GHASSAN ALASAAD, NADIA ALASAAD, SUHAIB ALLABABIDI, SIDD BIKKANNAVAR, JÉRÉMIE DUPIN, AARON GACH, ISMAIL ABDEL-RASOUL a.k.a. ISMA'IL KUSHKUSH, DIANE MAYE, ZAINAB MERCHANT, MOHAMMED AKRAM SHIBLY, and MATTHEW WRIGHT, Plaintiffs, v. KIRSTJEN NIELSEN, Secretary of the U.S. Department of Homeland Security, in her official capacity; KEVIN McALEENAN, Acting Commissioner of U.S. Customs and Border Protection, in his official capacity; and THOMAS HOMAN, Acting Director of U.S. Immigration and Customs Enforcement, in his official capacity, Defendants.	Civil Action No. 17-cv-11730-DJC Hon. Denise J. Casper

PLAINTIFFS' MEMORANDUM
IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

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

Other Authorities

Rules

INTRODUCTION

U.S. border officers searched the smartphones, laptops, and other electronic devices of more than 30,000 international travelers last year, more than triple the number from just two years earlier. Officers rummaged through these travelers' "privacies of life," *Riley v. California*, 134 S. Ct. 2473, 2495 (2014)—the vast quantities of emails, photographs, and other highly sensitive information that people store on their devices. Government policies expressly authorize officers to conduct these searches without a warrant or probable cause, and usually without even reasonable suspicion of wrongdoing. Plaintiffs are 11 travelers subjected to these policies and practices who have standing to seek injunctive and declaratory relief to avoid them in the future. Warrantless border searches of electronic devices violate the First and Fourth Amendments. The Fourth Amendment also prohibits confiscations of travelers' devices absent probable cause, for purposes of searching them after travelers leave the border.

BACKGROUND

A. Defendants' Policies and Practices.

Defendants, who are responsible for the challenged searches, seizures, practices, and policies, are the heads of the U.S. Department of Homeland Security ("DHS") and two of its component agencies, U.S. Customs and Border Protection ("CBP") and U.S. Immigration and Customs Enforcement ("ICE"). Amended Complaint, ECF No. 7 ("Am. Compl.") ¶¶ 3, 24–26. CBP and ICE have issued policies expressly authorizing the challenged searches and confiscations. These policies do not require a warrant or probable cause to believe that a device contains contraband or evidence of a violation of immigration or customs laws. *Id*. ¶ 1. They usually do not even require reasonable suspicion. *Id*. ¶¶ 1, 9, 57, 58.

CBP's 2009 policy authorized officers to "examine electronic devices" and "review and analyze the information encountered at the border"—"with or without individualized suspicion." *Id*. ¶¶ 8, 58. On January 4, 2018, after Plaintiffs filed the Amended Complaint, CBP's 2009 policy was superseded by CBP Directive No. 3340-049A. *See* Defendants' Notice of Supplemental Authority, ECF No. 18, at 1.[1]

CBP's 2018 policy never requires a warrant or probable cause for device searches at the border. Rather, for what it deems an "advanced search of an electronic device," it requires either "reasonable suspicion of activity in violation of the laws enforced or administered by CBP" or a "national security concern." Exhibit A to Defendants' Notice of Supplemental Authority, ECF No. 18-1 (CBP's 2018 policy at § 5.1.4). An "advanced search" is one "in which an Officer connects external equipment . . . to an electronic device . . . to review, copy, and/or analyze its contents." *Id.* The policy prohibits border officers from accessing cloud content. *Id.* at § 5.1.2. The policy allows any other device search (a "basic" search) "with or without suspicion." *Id*. at § 5.1.3. It thus permits searches without any individualized suspicion (1) when officers probe a device manually, irrespective of the invasiveness or duration of the search, or (2) when an "advanced search" implicates a "national security concern." *Id*. § 5.1.4. Finally, the policy does not apply to searches by ICE, even when CBP transfers devices to ICE for a search. *Id*. at § 2.7. CBP's new policy falls short of resolving the constitutional claims in this case.

ICE's policy, issued in 2009 and currently in force, authorizes ICE agents to search electronic devices "with or without individualized suspicion." Am. Compl. ¶¶ 8, 58; *see also*

[1] Plaintiffs respectfully request that this Court take judicial notice of CBP's 2018 policy, because its existence and contents are "fact[s] that [are] not subject to reasonable dispute." Fed. R. Evid. 201(b). Such judicial notice would not convert the pending motion to dismiss into a motion for summary judgment. *See Freeman v. Town of Hudson*, 714 F.3d 29, 36–37 (1st Cir. 2013).

Memorandum in Support of Defendants' Motion to Dismiss, ECF No. 15 ("Def. Br."), at 3–4. Unlike CBP's 2018 policy, ICE's policy does not prohibit cloud searches.

The CBP and ICE policies also permit lengthy confiscations of travelers' electronic devices. CBP's 2018 policy states that devices may be detained for on-site or off-site searches and that such detention "ordinarily" should not exceed five days, but can be prolonged with supervisory approval. ECF No. 18-1 (CBP's 2018 policy at §§ 5.4.1–5.4.1.1). ICE's policy expressly permits agents to confiscate devices without individualized suspicion for "further review" on-site or off-site. Am. Compl. ¶ 61. The default period of confiscation is 30 days, although ICE supervisors may extend this period under undefined "circumstances . . . that warrant more time." *Id*.

Under these policies, the number of border searches of electronic devices has grown rapidly. According to CBP data, CBP conducted 30,200 device searches in fiscal year 2017. Exhibit B to Defendants' Notice of Supplemental Authority, ECF No. 18-2, at 3 n.7. This is compared to just 8,503 searches in fiscal year 2015, Am. Compl. ¶ 38, meaning that the number of searches has more than tripled in only two years.

B. Border Searches and Confiscations of Plaintiffs' Devices.

All 11 Plaintiffs were subjected to border searches of their electronic devices without a warrant or probable cause to believe the devices contained contraband or evidence of a violation of immigration or customs laws. Am. Compl. ¶¶ 2, 37, 169. Four Plaintiffs also were subjected to prolonged device confiscation without probable cause: Ghassan and Nadia Alasaad, Suhaib Allababidi, and Matthew Wright. *Id*. ¶¶ 72, 80, 154, 173.[2]

[2] Mr. Allababidi's locked phone was returned to him after the filing of the Amended Complaint, on December 13, 2017, more than ten months after it was confiscated on January 21, 2017. *See* Def. Br. at 9 n.5; Am. Compl. ¶¶ 77, 79.

Electronic devices contain massive amounts of data, and their storage capacities continue to grow. Am. Compl. ¶ 30. Nearly everyone who crosses U.S. borders carries an electronic device of some kind, which can include mobile phones, laptops, tablets, digital cameras, and portable digital storage devices. *Id*. ¶ 27. These devices contain a diverse array of personal, expressive, and associational information that can span years of a person's life. *Id.* ¶¶ 31, 33, 34.

ARGUMENT

The motion to dismiss should be denied. Plaintiffs have standing to raise their claims that the Defendants' searches and seizures of electronic devices at the U.S. border violate the First and Fourth Amendments to the U.S. Constitution. Furthermore, Plaintiffs have adequately stated their claims. To survive a motion to dismiss, a complaint need only "'give the defendant fair notice of what the . . . claim is and the grounds upon which it rests,' and allege 'a plausible entitlement to relief.'" *Decotiis v. Whittemore*, 635 F.3d 22, 29 (1st Cir. 2011). The Court must accept the well-pleaded facts in the complaint as true and draw all reasonable inferences in favor of Plaintiffs. *See Gargano v. Liberty Int'l Underwriters, Inc.*, 572 F.3d 45, 48 (1st Cir. 2009).

I. Plaintiffs Have Standing to Seek Injunctive and Declaratory Relief.

Plaintiffs have standing to seek prospective equitable relief. Defendants' actions—searching and confiscating Plaintiffs' devices and retaining their data pursuant to Defendants' official policies and practices—violate Plaintiffs' constitutional rights and create a substantial risk that they will suffer these injuries again when crossing the U.S. border.

To establish Article III standing, a plaintiff must show: (1) an "injury in fact" that is "concrete and particularized" and "actual or imminent," not "conjectural" or "hypothetical"; (2) a "causal connection" between the injury and 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). To seek an injunction, a plaintiff must show "a sufficient likelihood that he will again be wronged in a similar way." *City of Los Angeles v. Lyons*, 461 U.S. 95, 111 (1983). This requires either a "'substantial risk' that the harm will occur" or a threat that is "certainly impending." *Reddy v. Foster*, 845 F.3d 493, 500 (1st Cir. 2017) (quoting *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014)).

Here, Plaintiffs allege two distinct injuries to their First and Fourth Amendment rights that entitle them to injunctive and declaratory relief. First, Plaintiffs face a "substantial risk" that their devices will again be searched and confiscated pursuant to Defendants' policies and practices. *See* Am. Compl. ¶ 156. Second, Defendants retain Plaintiffs' digital information gathered during past searches. *Id.* ¶ 157.[3] Defendants do not contest past injury, causality, or (for future searches) redressability.[4]

A plaintiff's burden varies with the stage of the proceedings. "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we 'presume that general allegations embrace those specific facts that are necessary to support the claim.'" *Lujan*, 504 U.S. at 561. In cases challenging law enforcement practices, as here, courts have denied motions to dismiss injunctive claims in part because of the early stage of proceedings, *i.e.*, before any discovery. *See, e.g.*, *McBride v. Cahoone*, 820 F. Supp. 2d 623, 633 (E.D. Pa. 2011) ("[W]e cannot conclude at this nascent stage of the proceedings that [plaintiff] lacks standing."); *Rodriguez v. Cal. Highway Patrol*, 89 F. Supp. 2d

[3] Plaintiffs' arguments for standing do not depend on the chill of their First Amendment rights. *Cf.* Def. Br. at 7, 9, 14–15. Rather, their standing is based on the injury to their rights from searches of their electronic devices pursuant to official policies and practices authorizing warrantless and suspicionless searches.

[4] Defendants returned Mr. Allababidi's phone two days before filing their Motion to Dismiss (Def. Br. at 9 n. 5), so he no longer seeks an injunction for its return. *Cf.* Am. Compl. Prayer ¶ H.

1131, 1142 (N.D. Cal. 2000) ("Plaintiffs are entitled to discovery to attempt to establish an evidentiary basis for their claims for injunctive relief.").[5]

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

Plaintiffs face a substantial risk of future injury because they will continue to be exposed to Defendants' adopted policies and practices authorizing border device searches and confiscations when Plaintiffs travel abroad.[6] Standing to seek prospective relief may rest on allegations that (1) the defendant adopted an unlawful policy or practice, and (2) the plaintiff will be exposed to it. *See Berner v. Delahanty*, 129 F.3d 20, 24 (1st Cir. 1997) (requiring "a realistic risk of future exposure to the challenged policy"). Moreover, four Plaintiffs were subjected to searches under Defendants' policies on multiple occasions, which makes abundantly clear that they face a heightened risk of such searches when they travel again. Finally, although Defendants contest standing based on the supposedly low odds any particular traveler will be searched, Def. Br. at 7, 10–11, they ignore clear precedents holding that Plaintiffs may assert standing by relying on increased risk of injury caused by Defendants.

[5] *See also Gordon v. City of Moreno Valley*, 687 F. Supp. 2d 930, 940 (C.D. Cal. 2009); *Bassette v. City of Oakland*, No. C–00–1645 JCS, 2000 WL 33376593, at *6 (N.D. Cal. Aug. 11, 2000); *Nat'l Cong. for Puerto Rican Rights v. City of New York*, 75 F. Supp. 2d 154, 164 (S.D.N.Y. 1999).

[6] The specific and plausible allegations here are distinguishable from the allegations in *Clapper v. Amnesty Int'l*, 568 U.S. 398 (2013), that the Court deemed speculative and attenuated. *Cf.* Def. Br. at 8–9, 11, 14–15. That case is relevant to pre-enforcement actions. The plaintiffs had sued to enjoin a statute granting the National Security Agency new surveillance powers—the day it went into effect. In that posture, the Court rejected standing, given the "highly attenuated chain of possibilities." *See Schuchardt v. President of the U.S.*, 839 F.3d 336, 338–39 (3rd Cir. 2016) (distinguishing *Clapper* on this basis); *Martin v. Evans*, 241 F. Supp. 3d 276, 283 (D. Mass. 2017) (same). Here, by contrast, Plaintiffs have already been subjected to searches pursuant to Defendants' policies, and face both ongoing injuries arising from those searches and a substantial risk of future injury.

1. Defendants Adopted the Challenged Policies and Practices.

Injured parties can show future injury when, as here, "[t]he offending policy remains firmly in place." *Dudley v. Hannaford Bros. Co.*, 333 F.3d 299, 306 (1st Cir. 2003); Am. Compl. ¶¶ 3, 8, 24–26, 57–61; *see also Berner*, 129 F.3d at 24; *Connor B. v. Patrick*, 771 F. Supp. 2d 142, 153 (D. Mass. 2011); *Ocasio v. City of Lawrence, Mass.*, 788 F. Supp. 99 (D. Mass. 1992). For example, courts recognize injunctive standing to challenge myriad police policies and practices. *See, e.g.*, *Mack v. Suffolk County*, 191 F.R.D. 16, 21 (D. Mass. 2000) (strip searches); *Deshawn E. by Charlotte E. v. Safir*, 156 F.3d 340, 344–45 (2d Cir. 1998) (interrogations); *Thomas v. County of Los Angeles*, 978 F.2d 504, 506–07 (9th Cir. 1992) (searches and seizures).[7]

This case is unlike *Lyons*, where the plaintiff did not allege that the government "ordered or authorized" the challenged policy or practice. 461 U.S. at 106–07 & n.7. Many cases distinguish *Lyons* on this basis. *See, e.g.*, *Am. Postal Workers Union v. Frank*, 968 F.2d 1373 (1st Cir. 1992); *Connor B.*, 771 F. Supp. 2d at 153; *Mack*, 191 F.R.D. at 21; *cf.* Def. Br. at 10.[8]

Regular enforcement further supports standing. "[T]he frequency of alleged injuries inflicted by the practices at issue . . . creates a likelihood of future injury sufficient to address any standing concerns." *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

[7] *See also LaDuke v. Nelson*, 762 F.2d 1318, 1324 (9th Cir. 1985); *Smith v. City of Chicago*, 143 F. Supp. 3d 741, 752 (N.D. Ill. 2015); *Morales v. Chadbourne*, 996 F. Supp. 2d 19, 38 (D.R.I. 2014); *Aichele v. City of Los Angeles*, 314 F.R.D. 478, 493 (C.D. Cal. 2013); *Ortega-Melendres v. Arpaio*, 836 F. Supp. 2d 959, 979, 985 (D. Ariz. 2011); *McBride*, 820 F. Supp. 2d at 635; *Aguilar v. ICE*, 811 F. Supp. 2d 803, 828 (S.D.N.Y. 2011); *Roe v. City of New York*, 151 F. Supp. 2d 495, 503 (S.D.N.Y. 2001); *Rodriguez*, 89 F. Supp. 2d at 1142; *Md. State Conference of NAACP Branches v. Md. Dep't of State Police*, 72 F. Supp. 2d 560, 564 (D. Md. 1999).

[8] Defendants also miss the mark with *Reddy v. Foster*, 845 F.3d 493 (1st Cir. 2017), which rejected pre-enforcement standing to challenge a criminal ban on protesting near clinics. *See* Def. Br. at 11. There, enforcement was impossible before a clinic marked its no-protest zone, which no clinic had done. But here, Defendants actively enforce the challenged policies and practices.

injunctive relief).[9] Here, device searches at the border are rampant—approximately 30,000 in fiscal year 2017—and their frequency more than tripled in just two years. *Supra* at 3.

2. Plaintiffs Will Be Exposed to the Challenged Policies and Practices.

Standing to seek prospective relief rests on a plaintiff's "realistic risk of future exposure to the challenged policy." *Berner*, 129 F.3d at 24 (lawyer had standing to challenge a judge's policy, though the lawyer might have had future cases assigned to 15 other judges). Plaintiffs need not prove they "inevitably will suffer" future injury. *Dimarzo v. Cahill*, 575 F.2d 15, 18 (1st Cir. 1978) (prisoners had standing to challenge fire hazards); *see also Cotter v. City of Boston*, 193 F. Supp. 2d 323, 337 (D. Mass. 2002) (employees "exposed" to workplace policy had standing to challenge it, despite uncertainty when it would next be applied), *rev'd in part on other grounds*, 323 F.3d 160 (1st Cir. 2003); *Connor B.*, 771 F. Supp. 2d at 150, 153 (children had standing based on their exposure to a foster agency's "systemic failures").[10]

Here, Plaintiffs have a "realistic risk of future exposure" to the challenged policies and practices. *See Berner*, 129 F.3d at 24. Plaintiffs "regularly travel outside the country with their electronic devices and intend to continue doing so." Am. Compl. ¶ 2. They travel abroad for work, to visit friends and family, and for vacation and tourism. *Id.* ¶¶ 62, 73, 77, 81, 86, 98, 105, 108, 114, 120, 126, 136, 143, 147. These allegations suffice on a motion to dismiss. *See, e.g.*, *Ibrahim v. DHS*, 669 F.3d 983, 993–94 (9th Cir. 2012) (plaintiff sufficiently pled standing to

[9] *See also*, *e.g.*, *Thomas*, 978 F.2d at 508; *Ligon v. City of New York*, 288 F.R.D. 72, 81 (S.D.N.Y. 2013); *Roe*, 151 F. Supp. 2d at 503; *Nat'l Cong.*, 75 F. Supp. 2d at 161.

[10] This case is unlike those that denied standing where the plaintiff was not exposed to the challenged policy. *Cf. Rumford Pharmacy, Inc. v. City of E. Providence*, 970 F.2d 996, 1001 (1st Cir. 1992) (plaintiff with no plan to acquire a liquor license could not challenge a license rule); *Brown v. Hot, Sexy & Safer Prods., Inc.*, 68 F.3d 525 (1st Cir. 1995) (student unlikely to view future school assemblies could not challenge risqué assemblies); *Blake v. Southcoast Health Sys., Inc.*, 145 F. Supp. 2d 126, 132 (D. Mass. 2001) (decedent faced no future harm at all).

challenge border screening policies). Plaintiffs are unlike those in *Lujan*, 504 U.S. at 564, who could not establish standing to seek prospective relief. *Cf.* Def. Br. at 12. Plaintiffs here allege ample past and future travel, while the plaintiffs in *Lujan* alleged only plans to return "some day" to isolated parts of the globe they had visited many years before. 504 U.S. at 564. And Defendants here move for pre-discovery dismissal, while the *Lujan* plaintiffs moved for post-discovery summary judgment.[11]

Additionally, Plaintiffs' conduct—traveling with electronic devices—is commonplace and innocent. Plaintiffs are exposed to warrantless, suspicionless search and confiscation policies and practices through no fault of their own. This further distinguishes this case from *Lyons*-type cases, where plaintiffs could theoretically avoid future injury by obeying the law and avoiding conflict with police. *See, e.g.*, *LaDuke*, 762 F.2d at 1326; *Smith*, 143 F. Supp. 3d at 752; *Cherri v. Mueller*, 951 F. Supp. 2d 918, 930 (E.D. Mich. 2013); *Ortega*, 836 F. Supp. 2d at 987; *Floyd*, 283 F.R.D. at 169–70; *Roe*, 151 F. Supp. 2d at 503; *Rodriguez*, 89 F. Supp. 2d at 1142; *Nat'l Cong.*, 75 F. Supp. 2d at 161.

Finally, 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). Here, each Plaintiff suffered at least one border device search, and four suffered a confiscation. Am. Compl. ¶¶ 37, 72, 80, 154. Plaintiffs are thus more likely than other travelers to suffer harms in the future. *Cf.* Def. Br. at 11–12, 15 n.6. First, when Plaintiffs next cross the border, Defendants' records will alert officers to the past searches and confiscations, which may increase the likelihood of repeated searches. *See, e.g.*, *Tabbaa v. Chertoff*, No. 05-CV-582S, 2005 WL 3531828, at *9 (W.D.N.Y. Dec. 22, 2005) (observing that information in government databases about prior border stops of

[11] At the Court's request, Plaintiffs will provide more detail of their recent and upcoming travel.

the plaintiffs "could be used to expand, enhance, or lengthen a border investigation" of them in the future). Second, whatever prompted officers to search Plaintiffs' devices may prompt future searches. And even if Plaintiffs faced the same odds as other travelers, "where a harm is concrete, though widely shared, the Court has found 'injury in fact.'" *FEC v. Akins*, 524 U.S. 11, 24 (1998).[12]

3. Four Plaintiffs Suffered Multiple Device Searches.

Additional facts buttress Plaintiffs' standing here: Mr. Kushkush suffered three border device searches, and Ms. Alasaad, Mr. Dupin, and Mr. Shibly each suffered two. Am. Compl. ¶¶ 68–70, 73–76, 90, 96, 107, 112, 117, 140, 146.[13] The "possibility of recurring injury ceases to be speculative when actual repeated incidents are documented." *Thomas*, 978 F.2d at 507; *Floyd*, 283 F.R.D. at 169. Thus, courts often rest standing for injunctive relief, in part, on multiple past applications to a plaintiff of the challenged law enforcement policy. *Stinson v. City of New York*, 282 F.R.D. 360, 382 (S.D.N.Y. 2012); *Smith*, 143 F. Supp. 3d at 752; *Morales*, 996 F. Supp. 2d at 37–38; *Cherri*, 951 F. Supp. 2d at 930; *Aguilar*, 811 F. Supp. 2d at 827; *Nat'l Cong.*, 75 F. Supp. 2d at 161.

To be clear, however, "there is no per se rule requiring more than one past act . . . as a basis for finding a likelihood of future injury." *Roe*, 151 F. Supp. 2d at 503; *see also Floyd*, 283 F.R.D. at 170 ("Even [a] single stop, in light of the tens of thousands of facially unlawful stops,

[12] Defendants' cases (Def. Br. at 12) do not suggest otherwise. In *Lujan*, the Court distinguished a "generally available grievance" shared by "the public at large," from "concrete injury [that] has been suffered by many persons," such as a mass tort. 504 U.S. at 572–74. The mass constitutional violations here are the latter. Defendants' language from *Conservation Law Foundation v. Reilly*, 950 F.2d 38, 41 (1st Cir. 1991), concerns organizational standing, which is not at issue here.

[13] During Ms. Alasaad's second search, officers demanded her phone (she didn't have it), seized from her bag the phone her 11-year-old daughter was using, told Ms. Alasaad to unlock it (she didn't know the password), and coerced her daughter into unlocking it. Am. Compl. ¶¶ 73–76.

would likely confer standing."); *Hernandez v. Cremer*, 913 F.2d 230, 235 (5th Cir. 1990); *Ligon*, 288 F.R.D. at 81 n.52; *Ortega*, 836 F. Supp. 2d at 987.

4. The Odds of Plaintiffs' Future Searches Suffice to Plead Standing.

Defendants argue that Plaintiffs lack standing to seek injunctive relief because the approximately 30,000 device searches in fiscal year 2017 by CBP involved only a small proportion of all border crossings. *See* Def. Br. at 7, 10–11. But courts have allowed people exposed to all manner of law enforcement policies and practices to seek injunctive relief, without regard to the odds of being subjected to them in the future. *See, e.g.*, *LaDuke*, 762 F.2d at 1324 (home searches); *Smith*, 143 F. Supp. 3d at 752 (sidewalk stops); *NAACP*, 72 F. Supp. 2d at 564 (traffic stops). As explained above, standing here rests soundly on Plaintiffs' exposure to Defendants' policies and practices. *See Ortega*, 836 F. Supp. 2d at 979 (motorists had standing to challenge stops policies, though the "likelihood that any particular named Plaintiff will again be stopped in the same way may not be high," due to the nature of their "exposure" to the policies).

Additionally, Plaintiffs' showing of probabilistic injury is sufficient to confer injunctive standing. "[P]robabilistic harms are legally cognizable." *Me. People's All. v. Mallinckrodt, Inc.*, 471 F.3d 277, 282, 283, 285 (1st Cir. 2006); *accord Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149 (4th Cir. 2000) (en banc); *Arcia v. Florida Sec'y of State*, 772 F.3d 1335, 1341 (11th Cir. 2014). In other words, "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) (emphasis added). "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); *see also Kerin v. Titeflex Corp.*, 770 F.3d 978, 983 (1st Cir. 2014) ("[A] small probability of a great harm may

be sufficient."). Here, the harm is severe: government snooping through vast reservoirs of our most private information. Myriad kinds of probabilistic harm support injunctive standing. *See, e.g.*, *NRDC v. EPA*, 464 F.3d 1, 7 (D.C. Cir. 2006) (1 in 200,000 odds of skin cancer); *Sierra Club v. Mainella*, 459 F. Supp. 2d 76, 93 (D.D.C. 2006) (1 in 10,000 odds of an oil well fire); *Mountain States Legal Found.*, 92 F.3d at 1234 (5.4% reduction of wildfire fuel, instead of 14.2%).

Likewise, Plaintiffs' risk of probabilistic harm is not, as Defendants contend, "far-fetched," "miniscule," or "vanishingly small." *See* Def. Br. at 7, 11, 12. Border device searches occur regularly and with increasing frequency, more than trebling in two years to about 30,000 per year. *Supra* at 3. There is no doubt that Defendants' policies and practices expose Plaintiffs to an increased risk of future harm.[14]

B. Plaintiffs Have Standing to Seek Expungement.

Defendants' retention of information obtained from the illegal searches of Plaintiffs' devices provides an additional ground for standing. If law enforcement improperly collects information about a person, the continued retention of that information is an ongoing injury, and a demand to expunge it supports standing to seek prospective relief. *See Tabbaa v. Chertoff*, 509 F.3d 89, 96 & n.2 (2d Cir. 2007) ("[P]laintiffs possess Article III standing based on their demand for expungement."); *Hedgepeth v. WMATA*, 386 F.3d 1148, 1152 (D.C. Cir. 2004); *Paton v. La Prade*, 524 F.2d 862, 868 (3rd Cir. 1975); *Fox v. District of Columbia*, 851 F. Supp. 2d 20, 29

[14] In *Abidor v Napolitano*, 990 F. Supp. 2d 260, 270–73 (E.D.N.Y. 2013), the court erroneously rejected the probabilistic approach, and denied standing to challenge border device searches, resting on the claimed 1-in-100,000 odds of a search. (The odds now are 1 in 10,000, according to CBP's FY 2017 statistics indicating a 0.008% search rate. Def. Br. at 10–11.) Moreover, *Abidor* is distinguishable: the court assumed, absent record evidence, that officers will not search without reasonable suspicion, 990 F. Supp. 2d at 271–72; but Plaintiffs here allege searches absent reasonable suspicion or any modicum of suspicion at all, *see* Am. Compl. ¶¶ 1, 9, 57–59, 156(c). Also, Plaintiffs here seek a warrant requirement to search devices. *Cf.* Def. Br. at 12.

(D.D.C. 2012). Here, Plaintiffs challenge Defendants' unlawful retention of information seized from their devices, Am. Compl. ¶ 157, and they seek expungement of that information, *id.* at Prayer ¶ I. This establishes standing, independent of the substantial risk of future border device searches and confiscations.

Plaintiffs have pled specific and plausible facts showing retention. *See Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009); *cf.* Def. Br. at 7, 13. Each Plaintiff suffered a border device search. Am. Compl. ¶ 2. Defendants' policies expressly authorize retention of data obtained from device searches. Am. Compl. ¶ 82(b); *id*. at ¶ 8 (CBP's 2009 policy at § 5.4.1.2 and ICE's 2009 policy at § 8.5(1)(b)); ECF No. 18-1 (CBP's 2018 policy at § 5.5). Defendants' own records reveal officers retained information from Mr. Wright: they extracted information from his devices; they did not document its destruction; and their policies require such documentation. Am. Compl. ¶ 155.[15]

Expungement will redress a serious harm. *Cf.* Def. Br. at 13–14. Defendants' ongoing retention of this information compounds the violations of Plaintiffs' Fourth Amendment rights, because Defendants remain free to use and exploit it or share it with other agencies that may do the same. *See* ECF No. 18-1 (CBP's 2018 policy at § 5.5.1.3–5.5.1.4). Expungement will end this injury. Defendants mistakenly rely on criminal cases about the exclusionary rule that do not show otherwise. *See Herring v. United States*, 555 U.S. 135 (2009); *Pa. Bd. of Parole v. Scott*, 524 U.S. 357 (1998).

[15] Defendants err in demanding Plaintiffs provide evidence of data retention similar to that obtained by Mr. Wright via a Freedom of Information Act request. Def. Br. at 13. As explained above, all Plaintiffs have established sufficient facts to plausibly demonstrate that Defendants retained their data when officers searched their devices, which is all that is required at the pleading stage. *Cf. Hochendoner v. Genzyme Corp.*, 823 F.3d 724, 731 (1st Cir. 2016).

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

The unprecedented privacy interests Plaintiffs possess in the contents of their cell phones, laptops, and other personal electronic devices make warrantless, suspicionless border searches of those devices unconstitutional. Electronic devices are unlike any other physical containers, given their "immense storage capacity" and the "highly personal" nature of the information they contain. *Riley*, 134 S. Ct. at 2489–90; *United States v. Wurie*, 728 F.3d 1, 8 (1st Cir. 2013), *aff'd*, *Riley*, 134 S. Ct. 2473. The Fourth Amendment's warrant requirement was enacted precisely to safeguard the kinds of privacy interests implicated by these searches. Separately, under the Supreme Court's border cases, searches of electronic devices without a warrant or probable cause are constitutionally unreasonable. To rule otherwise would give the government unfettered access to "a virtual warehouse" of the most intimate aspects of Plaintiffs' lives simply because they have decided to travel internationally. *See Wurie*, 728 F.3d at 9.

A. Border Searches of Electronic Devices Violate the Fourth Amendment Absent a Warrant Based on Probable Cause.

1. The Supreme Court's Analysis in *Riley v. California* Dictates That a Warrant Is Required.

In *Riley v. California*, the Supreme Court made clear that traditional exceptions to the Fourth Amendment's warrant requirement do not automatically extend to searches of digital data. Rather, in determining whether a warrant exception applies to a particular "category of effects," the Constitution requires balancing individual privacy interests against legitimate governmental interests. *Riley*, 134 S. Ct. at 2484–85. *Riley* held that the search-incident-to-arrest exception does not apply to cell phones for two reasons: first, individuals have unique privacy interests in the contents of cell phones; and second, warrantless searches of cell phones are not sufficiently "tethered" to the underlying rationales for the search-incident-to-arrest exception

because they are not necessary to ensure officer safety or preserve evidence. *See id*. at 2484–85. The same reasoning applies here and leads to the same conclusion. The privacy interests travelers have in the contents of their electronic devices are identical to those in *Riley*, and warrantless searches of electronic devices are not justified by the limited purposes of the border search exception, which is immigration and customs enforcement.

That government searches of electronic devices occur at the border does not alter the analysis. The border search exception to the Fourth Amendment's warrant and probable cause requirements has always been subject to constitutional limits. As the Supreme Court held in *United States v. Ramsey*, "[t]he border-search exception is grounded in the recognized right of the sovereign to control, *subject to substantive limitations imposed by the Constitution*, who and what may enter the country." 431 U.S. 606, 620 (1977) (emphasis added). Thus, the border search exception—which permits warrantless and often suspicionless searches, *see United States v. Montoya de Hernandez*, 473 U.S. 531 (1985)—does not extend to electronic devices, and officers must obtain a warrant to search their contents.[16]

a. Travelers Have Extraordinary Privacy Interests in the Digital Data Their Electronic Devices Contain.

It is difficult to overstate the magnitude of the privacy interests that Plaintiffs, like all travelers, have in the contents of their personal electronic devices. Border searches of personal property, like searches incident to arrest, are usually "limited by physical realities and tend[] as a general matter to constitute only a narrow intrusion on privacy," *Riley*, 134 S. Ct. at 2489.

[16] Defendants wrongly rely on *Riley*'s mention of "case-specific exceptions" to the warrant requirement such as exigent circumstances. *See* Def. Br. at 19. Nothing in *Riley* forecloses applying its analysis to other categorical exceptions to the warrant requirement such as the border search exception. *See Riley*, 134 S. Ct. at 2484 (the search-incident-to-arrest exception is a "categorical rule"); *Ramsey*, 431 U.S. at 621 (the border search exception is "similar" to the search-incident-to-arrest exception).

Border searches of modern electronic devices, however, reveal the "sum of an individual's private life," *id.*, and "bear[] little resemblance" to searches of travelers' luggage, *id.* at 2485; *see also Wurie*, 728 F.3d at 9 ("[I]ndividuals today store much more personal information on their cell phones than could ever fit in a wallet, address book, [or] briefcase."); *United States v. Kim*, 103 F. Supp. 3d 32, 55 (D.D.C. 2015). The fact that luggage may contain some physical items with personal information does not negate the unique privacy interests in electronic devices. *See Riley*, 134 S. Ct. at 2493.

Riley held that electronic devices differ fundamentally—in quantitative and qualitative senses—from physical containers. *Id*. at 2489; *see also* Am. Compl. ¶¶ 29–35.[17]

Quantitatively, with their "immense storage capacity," electronic devices can contain "millions of pages of text, thousands of pictures, or hundreds of videos." *Riley*, 134 S. Ct. at 2489; *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."). A border search of an electronic device is like a bag search that "could reveal not only what the bag contained on the current trip, but everything it had ever carried." *Cotterman*, 709 F.3d at 965. As the *Riley* Court stated, this "gulf between physical practicability and digital capacity will only continue to widen in the future." 134 S. Ct. at 2489.

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."

[17] Defendants' focus on *Montoya de Hernandez* is misguided. *See* Def. Br. at 18. The Court's holding was limited to the context of alimentary canal drug smuggling, and it had no occasion to assess the balance of interests where vast amounts of private information are at issue.

Wurie, 728 F.3d at 8. Electronic devices "collect[] in one place many distinct types of information . . . that reveal much more in combination than any isolated record." *Riley*, 134 S. Ct. at 2489. The data on electronic devices can reveal our political affiliations, religious beliefs and practices, sexual and romantic lives, financial status, health conditions, and family and professional associations.[18] Indeed, searches of electronic devices "expose to the government far *more* than the most exhaustive search of a house"—a device such as a cell phone "not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Riley*, 134 S. Ct. at 2491 (emphasis in original); *see also Cotterman*, 709 F.3d at 964 (electronic devices "are simultaneously offices and personal diaries" and "contain the most intimate details of our lives").

b. Defendants' Interests Must Be Assessed in Light of the Narrow Purposes of the Border Search Exception.

The government's interests in searching the contents of electronic devices at the border without a warrant and probable cause are considerably more limited than Defendants contend. Under the *Riley* balancing test, the government's interests are analyzed by considering whether warrantless searches of a category of property are "tethered" to the narrow purposes justifying the warrant exception. *See Riley*, 134 S. Ct. at 2485; *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"); *Wurie*, 728 F.3d at 9 (warrantless searches must be "commensurate" with the purposes of the exception). Here, warrantless searches of electronic devices are not sufficiently tethered to the narrow purposes justifying the border search

[18] *Riley* requires a warrant to search the cell phone of an arrestee, even though the Court considered an arrestee to have "diminished privacy interests." 134 S. Ct. at 2488. Of course, the vast majority of international travelers are not suspected of any crime.

exception: immigration and customs enforcement. That is, warrantless border searches of electronic devices do not sufficiently advance these goals.[19] *See Montoya de Hernandez*, 473 U.S. at 537; *Carroll v. United States*, 267 U.S. 132, 154 (1925); *Boyd v. United States*, 116 U.S. 616, 624 (1886); *Cotterman*, 709 F.3d at 956 (emphasizing "narrow" scope of border search exception).

As with the search-incident-to-arrest exception, where warrantless and suspicionless searches are justified by the limited goals of protecting officer safety and preventing the destruction of evidence, the border search exception may "strike[] the appropriate balance in the context of physical objects" such as luggage, but its underlying rationales do not have "much force with respect to digital content on cell phones" or other electronic devices. *Cf. Riley*, 134 S. Ct. at 2484. Border officers determine a traveler's immigration status and authority to enter the United States by questioning travelers and inspecting official documents such as passports and visas, and officers enforce customs laws by searching travelers' luggage, vehicles, and, if necessary, their persons. *See, e.g.*, *United States v. Flores-Montano*, 541 U.S. 149, 151 (2004); *United States v. Molina-Gomez*, 781 F.3d 13, 16–17 (1st Cir. 2015). Just as the *Riley* Court stated that "data on the phone can endanger no one," 134 S. Ct. at 2485, physical items subject to customs laws cannot be hidden in digital data.[20]

[19] Whatever statutory authority Congress has given Defendants to enforce laws at the border, *see* Def. Br. at 2, those laws and the officers who enforce them are subject to constitutional limits.

[20] Two district courts recognized this weak tethering. In *United States v. Molina-Isidoro*, a drug smuggling case, the court stated that a warrantless search of "the contents of a cell phone does not seem to directly contribute to [one] justification for the border search exception—i.e., preventing the entry of unwanted illicit substances into the country." 267 F. Supp. 3d 900, 920 n.10 (W.D. Tex. 2016). In *United States v. Kolsuz*, 185 F. Supp. 3d 843, 858 (E.D. Va. 2016), an unlicensed firearms export case, the court stated that digital data "is merely indirect evidence of the things an individual seeks to export illegally—not the things themselves—and therefore the government's interest in obtaining this information is less significant than the government's

Some digital content, such as child pornography, may be considered "digital contraband" to be interdicted at the border. Def. Br. at 20; *cf. United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376–77 (1971). However, unlike physical contraband, digital contraband can easily be transported across borders via the internet. Additionally, digital contraband that is located solely in the cloud cannot be considered to be crossing the border and therefore subject to a border search. *See Riley*, 134 S. Ct. at 2491 (the search-incident-to-arrest exception "may not be stretched to cover a search of files accessed remotely" because that "would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house").[21] Thus, the government cannot demonstrate that any digital contraband that might be physically resident on travelers' devices is a significant or "prevalent" problem (in the words of the *Riley* Court) *at the border* that justifies or necessitates a *categorical rule* permitting warrantless border searches of electronic devices for every traveler entering or exiting the country. *Cf. Riley*, 134 S. Ct. at 2485–86 (noting insufficient evidence that warrantless searches of arrestees' cell phones would meaningfully protect officer safety or prevent the destruction of evidence and that, in any event, any such possibilities do "not justify dispensing with the warrant requirement across the board"); *Wurie*, 728 F.3d at 13 (holding that a warrantless cell phone search is not "necessary" to advance the goals of the search-incident-to-arrest warrant

---

interest in directly discovering the items to be exported illegally." The *Kolsuz* court concluded that "any digital information contained on a cell phone that is relevant to exporting goods illegally can be easily obtained once a border agent establishes some level of individualized suspicion." *Id.* Similarly, Defendants' reference to "information regarding the inadmissibility of prohibited goods or persons," Def. Br. at 20, is "not the things themselves." *Kolsuz*, 185 F. Supp. 3d at 858; *see also Boyd*, 116 U.S. at 623 ("The search for and seizure of . . . goods liable to duties and concealed to avoid the payment thereof, are totally different things from a 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.").

[21] Unlike CBP's 2018 policy, ICE's 2009 policy arguably permits border searches of cloud content. *See supra* at 2.

exception). Of course, where border officers have actual probable cause to believe contraband data is stored on a device, they can secure a search warrant. And in rare instances where there is truly no time to go to a judge, the exigent circumstances exception may apply. *See Riley*, 134 S. Ct. at 2486.

Even assuming that conducting warrantless device searches at the border might sometimes advance the government's goals of immigration and customs enforcement, the extraordinary privacy interests Plaintiffs and other travelers have in their electronic devices outweigh any governmental interests. *See United States v. Caballero*, 178 F. Supp. 3d 1008, 1017 (S.D. Cal. 2016) (stating that "[i]f it could, this Court would apply *Riley*," but recognizing it was bound by *Cotterman*). As a result, the Fourth Amendment requires that border officers must obtain a warrant before searching electronic devices.

2. Under the Supreme Court's Border Cases, Warrantless Searches of Electronic Devices are Unreasonable.

Even without reference to the Court's ruling in *Riley*, border search precedent provides a parallel justification for requiring a warrant based on probable cause for border searches of electronic devices. The Supreme Court has held that the scope of the border search exception to the warrant requirement is not unlimited, and that "[t]he Fourth Amendment commands that searches and seizures [at the border] be reasonable." *Montoya de Hernandez*, 473 U.S. at 537. As in other contexts, "[w]hat is reasonable depends upon all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself." *Id.* For example, the Court has left "open the question 'whether, and under what circumstances, a border search might be deemed "unreasonable" because of the particularly offensive manner in which it is carried out.'" *Flores-Montano*, 541 U.S. at 154 n.2 (quoting *Ramsey*, 431 U.S. at 618 n.13). Lower courts also have recognized that particularly "intrusive" or "offensive" searches at the border may "be

deemed unreasonable under the Fourth Amendment." *E.g.*, *United States v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008).

Warrantless border searches of devices cross the line that the Supreme Court contemplated and violate the Fourth Amendment's reasonableness requirement. First, as explained above, *see supra* Part II.A.1, these searches intrude upon the substantial individual privacy interests that travelers have in their electronic devices. *Ramsey* underscores the scale of those interests, even at the border. It distinguished the search of a vessel or container from the search of a house—which, the Court noted, required a warrant even before the ratification of the Constitution, 431 U.S. at 617—and it observed that "a port of entry is not a traveler's home." *Id.* at 618. Of course, a search of a cell phone "would typically expose to the government far *more* than the most exhaustive search of a house." *See Riley*, 134 S. Ct. at 2491 (emphasis in original).

Second, device searches at the border raise grave First Amendment concerns that affect the reasonableness analysis. *See infra* Part IV. In *Ramsey*, the Court left open the possibility that where First Amendment rights are implicated by a border search, the "full panoply" of Fourth Amendment protections—*i.e.* a warrant requirement—might apply. 431 U.S. at 623–24 & n.18.

Third, device searches at the border are often conducted in a "particularly offensive manner." *See Flores-Montano*, 541 U.S. at 154 n.2. As Plaintiffs' experiences demonstrate, officers can and do use threats of confiscation to extract device passcodes from travelers, search the devices' content for lengthy periods outside the travelers' presence, retain the contents of the devices, and even use physical force to seize devices. Am. Compl. ¶¶ 82, 155, 157.

Requiring a warrant for border device searches is both feasible and necessary to satisfy the requirement of reasonableness under the Fourth Amendment. *See Riley*, 134 S. Ct. at 2493

("Recent technological advances . . . have . . . made the process of obtaining a warrant itself more efficient."). The Supreme Court has contemplated this warrant process at the border. *See Ramsey*, 431 U.S. at 623–24; *Montoya de Hernandez*, 473 U.S. at 547 & n.13.[22]

B. At a Minimum, the Fourth Amendment Requires Heightened Suspicion for Border Searches of Electronic Devices.

If this Court holds that no warrant is required for border searches of electronic devices, it should hold that border officers must have probable cause. *Cf. California v. Acevedo*, 500 U.S. 565, 579–80 (1991) (although automobile searches do not require a warrant, they do require probable cause). A probable cause threshold is necessary to limit the massive privacy intrusion inflicted by device searches. *Cf. id.* at 574–76 (considering the differential benefits to privacy in certain rules over others before determining what is reasonable under the Fourth Amendment).

A probable cause requirement is consistent with the Supreme Court's border decisions. Contrary to Defendants' argument, *see* Def. Br. at 18, the Court has never suggested that the reasonable suspicion it required in *Montoya de Hernandez* is a ceiling for every border search, or that property searches might not require heightened protections. *See Flores-Montano*, 541 U.S. at

[22] Defendants' cases (Def. Br. at 17–19) do not diminish the Fourth Amendment's warrant requirement for border device searches. Some of these cases preceded *Riley*. *See United States v. Hampe*, No. 07-3-B-W, 2007 WL 1192365 (D. Me. Apr. 18, 2007); *House v. Napolitano*, No. 11-10852-DJC, 2012 WL 1038816 (D. Mass. Mar. 28, 2012). Others, from the Ninth Circuit, are bound by *Cotterman*, which itself preceded *Riley*. *See United States v. Mendez*, No. CR-16-00181-001-TUC-JGZ (JR), 2017 WL 928460 (D. Ariz. Mar. 9, 2017); *United States v. Cano*, 222 F. Supp. 3d 876 (S.D. Cal. 2016); *United States v. Ramos*, 190 F. Supp. 3d 992 (S.D. Cal. 2016); *United States v. Lopez*, No. 13-CR-2092 WQH, 2016 WL 7370030 (S.D. Cal. Dec. 20, 2016); *United States v. Hernandez*, No. 15-CR-2613-GPC, 2016 WL 471943 (S.D. Cal. Feb. 8, 2016). One is an unpublished, non-precedential appellate decision comprising a few unpersuasive sentences. *See United States v. Escarcega*, 685 Fed. Appx. 354 (5th Cir. 2017). The remainder are also unpersuasive for the reasons set forth above. *See Kolsuz*, 185 F. Supp. 3d 843; *United States v. Feiten*, No. 15-20631, 2016 WL 894452 (E.D. Mich. Mar. 9, 2016); *Abidor v. Johnson*, No. 10-CV-4059 (ERK), 2016 WL 3102017 (E.D.N.Y. June 2, 2016); *Molina-Isidoro*, 267 F. Supp. 3d 900; *United States v. Blue*, No. 1-14-CR-244-SCJ, 2015 WL 1519159 (N.D. Ga. Apr. 1, 2015); *United States v. Saboonchi*, 48 F. Supp. 3d 815 (D. Md. 2014).

152 (declining to decide "what level of suspicion" would be required for highly intrusive searches); *see also House v. Napolitano*, No. 11-10852-DJC, 2012 WL 1038816, at *7 (D. Mass. Mar. 28, 2012) (noting the "Supreme Court has not explicitly held that all property searches" never require suspicion). Rather, the Court's decisions establish reasonable suspicion as the *floor* for highly intrusive searches.

A probable cause requirement is necessary because device searches are highly intrusive and implicate core First and Fourth Amendment concerns. *See supra* Part II.A.1; *infra* Part IV. The weight of these harms will continue to grow as the government's technological ability to search devices becomes more powerful. "It is little comfort to assume that the government—for now—does not have the time or resources to seize and search the millions of devices that accompany the millions of travelers who cross our borders. It is the potential unfettered dragnet effect that is troublesome." *Cotterman*, 709 F.3d at 966.

Moreover, at the very least, courts have required reasonable suspicion for highly intrusive searches. *See Flores-Montano*, 541 U.S. at 152 (singling out "highly intrusive searches" that impact the "dignity and privacy interests" of travelers*)*; *United States v. Braks*, 842 F.2d 509, 511 & n.12 (1st Cir. 1988) (one factor in assessing a search's "degree of invasiveness or intrusiveness" is whether it abrogates reasonable expectations of privacy).[23] Device searches are extraordinarily invasive. *Supra* Part II.A.1; *see also Riley*, 134 S. Ct. at 2489; Am. Compl. ¶¶ 1, 9, 57–59 (alleging that the challenged policies authorize suspicionless border searches of electronic devices); *id*. at ¶ 156(c) (alleging that Plaintiffs are at risk of such searches). Thus,

[23] The First Circuit in *Braks*, 842 F.2d at 512 & n.12, cited *Winston v. Lee*, 470 U.S. 753, 762 (1985), which provided examples of intrusions (such as eavesdropping and home searches) that are not intrusions on the body but nonetheless "damage the individual's sense of personal privacy and security." Device searches are at least as intrusive, because they reveal "far *more* than the most exhaustive search of a house." *Riley*, 134 S. Ct. at 2491 (emphasis in original).

searches of electronic devices at the border are "non-routine" and require at least reasonable suspicion. *Cf. Montoya de Hernandez*, 473 U.S. at 541.

Finally, there is no valid distinction between manual and forensic searches, because both severely harm privacy by accessing essentially the same trove of highly personal information. Before *Riley*, the Ninth Circuit in *Cotterman* required reasonable suspicion for a forensic search and no suspicion for a manual search. 709 F.3d at 967–68. But that distinction has become legally and technologically untenable. Given the increasing volume and detail of personal information in electronic devices, and the growing ease of manually navigating them, manual searches are extraordinarily invasive of travelers' privacy. Am. Compl. ¶ 41. Without special training or equipment, a border officer can easily conduct thorough manual searches, including by opening and perusing various stored files, programs, and apps, or by using a device's built-in search function. *Id*. Indeed, the unlawful warrantless cell phone searches in *Riley* were manual. *See* 134 S. Ct. at 2480–81, 2493; *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'").[24] Thus, even if this Court were to accept the government's erroneous assertion that border searches can *never* require more than reasonable suspicion, Def. Br. at 18, there is no basis for requiring a level of suspicion for some device searches but not others, as CBP's 2018 policy does.

C. Adequate Cause to Search Must Be Tied to Data on the Electronic Device.

Given the substantial privacy and First Amendment interests at stake whenever the government searches the contents of electronic devices, adequate cause to search must require a

[24] During a manual search, officers can also review cloud-based content. Am. Compl. ¶ 42. While CBP's 2018 policy does not permit cloud searches, *see* ECF No. 18-1 (at § 5.1.2), ICE does not have a comparable policy. Moreover, *Riley* weighed the additional privacy harms of potential cloud searches, even if government "protocols" would prohibit them. 134 S. Ct. at 2491.

showing that data on the device indicates a violation of an immigration or customs law. This limitation is necessary to ensure that such searches do not constitute an end-run around Fourth Amendment prohibitions on general warrants. In other device search contexts, courts have required or assumed that probable cause must be tied to information to be found on the device. *See Wurie*, 728 F.3d at 13; *United States v. Griffith*, 867 F.3d 1265, 1274 (D.C. Cir. 2017). Any other rule would enable border officers to conduct dragnet device searches even when they have no reason to believe that relevant evidence of wrongdoing will be found on the device itself.

III. Confiscations of Electronic Devices Without Probable Cause After a Traveler Has Left the Border Violate the Fourth Amendment.

The Fourth Amendment requires that any confiscation of a traveler's electronic device be justified at its inception and reasonable in scope and duration. *See United States v. Place*, 462 U.S. 696, 701, 709–10 (1983).

Confiscation of an electronic device once a traveler leaves the border must be based on at least the level of suspicion needed for the search—in this case, probable cause (as required to get a warrant). *See supra* Part II.A. Any lesser standard is unreasonable, because it would permit confiscations where a subsequent search is not permitted. *Place*, 462 U.S. at 701 ("Where law enforcement 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.").

Additionally, the length of time a device is confiscated must be reasonable. *See House*, 2012 WL 1038816, at *9 (discussing *Place*). When considering the level of suspicion necessary to justify a seizure, courts have considered the duration of the seizure as an "important factor." *See Place*, 462 U.S. at 709. In *Place*, the Court held that the detention of a domestic traveler's

luggage for 90 minutes without probable cause violated the Fourth Amendment. *Id*. at 708; *see also United States v. Mitchell*, 565 F.3d 1347, 1351 (11th Cir. 2009) (noting that computers have become indispensable in everyday life, and so a 21-day delay in securing a warrant for a computer search was unreasonable). In the border search context, courts also consider the length of seizure to determine reasonableness. *See Molina-Gomez*, 781 F.3d at 20 (suggesting that reasonable suspicion was required for a 22-day border confiscation of a laptop); *United States v. Laich*, No. 08-20089, 2010 WL 259041, at *1 (E.D. Mich. Jan. 20, 2010) (a permanent seizure of a laptop at the airport, and its transportation hundreds of miles away, required probable cause).

CBP's 2009 and 2018 policies, and ICE's 2009 policy, do not satisfy these requirements because they permit confiscations of electronic devices to be searched after a traveler has left the border with no requirement of individualized suspicion, and with no effective limit on the amount of time the devices may be detained. *See supra* at 3. Furthermore, the prolonged confiscations of the devices of Plaintiffs Ghassan and Nadia Alasaad (approximately 15 days for two unlocked phones), Allababidi (over 10 months), and Wright (56 days) were not based on probable cause. These confiscations also were unreasonable in scope, because they included unlocked devices that could have been searched at the border, and unreasonable in duration, because they were not reasonably related to the length of time necessary to search locked phones. *See* Am. Compl. ¶¶ 65, 70, 72, 80, 164, 173; *see also House*, 2012 WL 1038816, at *3–*9 (holding a 49-day seizure of a locked laptop, USB device, and camera raised a plausible claim). Strikingly, Defendants returned Mr. Allababidi's phone to him only two days before filing their motion to dismiss this case. *See* Def. Br. at 9 n.5. This suggests Defendants had no real need to confiscate the phone for as long as 10 months.

IV. Warrantless, Suspicionless Searches of Electronic Devices Violate the First Amendment.

Defendants violate the First Amendment by searching the contents of electronic devices at the border without a warrant based on probable cause, or without any individualized suspicion.

Courts have long recognized that government demands for information revealing expressive activities burden First Amendment rights and require greater protections. *See, e.g.*, *Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 544 (1963). The government must have a compelling interest in the information and use narrowly tailored means that do not seek more information than necessary. *See, e.g.*, *id.* at 546 (prohibiting a subpoena to the NAACP from a legislative committee); *United States v. Rumely*, 345 U.S. 41, 46 (1953) (holding that the First Amendment limited a congressional committee's power to issue a subpoena to a bookseller seeking names of those who had purchased political publications); *Bursey v. United States*, 466 F.2d 1059, 1083 (9th Cir. 1972) (requiring substantial and immediate government interests in the information sought by a grand jury about a newspaper, and a means of obtaining it that was "not more drastic than necessary").

Defendants' regime of device searches at the border operates as a dragnet, allowing government agents to gather information in violation of numerous rights protected by the First Amendment. These include (1) the "freedom to engage in association for the advancement of beliefs and ideas," *see NAACP v. Alabama*, 357 U.S. 449, 460 (1958); (2) the right to speak anonymously, including online, *see McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995); *McMann v. Doe*, 460 F. Supp. 2d 259, 266 (D. Mass. 2006); (3) the right to receive and communicate ideas, including unpopular ones, *see, e.g.*, *Lamont v. Postmaster Gen.*, 381 U.S. 301 (1965); and (4) the right to read books or watch movies privately, *see, e.g.*, *Amazon.com LLC v. Lay*, 758 F. Supp. 2d 1154, 1167–70 (W.D. Wash. 2010); *In re Grand Jury Investigation*

of Possible Violation of 18 U.S.C. § 1461, 706 F. Supp. 2d 11, 17–18 (D.D.C. 2009). Press freedom is also burdened when the government has unfettered access to the identity of journalists' sources, the contents of journalists' communications, and journalistic work product, without legitimate justification. *See, e.g.*, *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) (holding courts cannot automatically grant demands for journalist work product because "unlimited or unthinking allowance of such requests will impinge upon First Amendment rights").

Plaintiffs' personal, privileged, confidential, and anonymous communications and associations may be reviewed and retained by the government under the challenged policies and practices, thereby impinging their First Amendment rights. Am. Compl. ¶¶ 46, 162. Furthermore, this massive government intrusion on communications privacy may chill Plaintiffs and other travelers from exercising their First Amendment rights. *Id*.

When a government search implicates First Amendment rights, a warrant based on probable cause is the appropriate remedy. *See, e.g.*, *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (holding that First Amendment interests endangered by a newsroom search could be protected by applying Fourth Amendment standards for a warrant with "scrupulous exactitude"); *New York v. P.J. Video, Inc.*, 475 U.S. 868, 877–78 (1986) (holding that a warrant was an adequate constitutional safeguard for a search of expressive materials).[25] Some courts have, in

[25] *See also* Michael Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. Natl. Sec. L. & Policy 247, 249, 250 (2015) (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 there is a "chilling effect," and "a warrant supported by probable cause will, in most cases, suffice to satisfy the narrow tailoring requirement").

fact, required enhanced First Amendment standards for search warrants. *See, e.g.*, *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. 2002) (en banc); *A Quantity of Copies of Books v. Kansas*, 378 U.S. 205 (1964).

The fact that the challenged device searches take place at the border does not vitiate the application of First Amendment scrutiny and the remedy of a warrant. In *Ramsey*, the Court recognized that First Amendment-protected speech might be chilled by customs searches of incoming international mail. While the Court declined to invalidate the existing statutory search regime, which allowed for searches where there was reason to believe the envelopes contained physical items, it notably did so because of regulations "flatly prohibit[ing], under all circumstances," customs officials from reading correspondence without a warrant. *Ramsey*, 431 U.S. at 623. The Supreme Court explicitly left open whether, "in the absence of the existing statutory and regulatory protection," "the appropriate response [to a chill on speech] would be to apply the full panoply of Fourth Amendment requirements." *Id* at 624 & n.18. The Court thus recognized that a warrant could protect the First Amendment rights at stake—even at the border.

Defendants cite *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005), and *United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008), in arguing against "a First Amendment exception to the border search doctrine." Def. Br. at 21. To the extent those cases considered the First Amendment implications of device searches, they are distinguishable, because they rested on factual assumptions that do not reflect the government's subsequent device search policies, practices, and capabilities. In *Ickes*, the court deemed it "far-fetched" that any traveler could be subjected to a search of their laptop because agents have "neither the time nor resources" to do so. 393 F.3d at 507. Moreover, the court assumed that any device search would likely take place—as it did in *Ickes*—only because of a traveler's conduct or after physical contraband had

been discovered. *Id.* The *Arnold* court explicitly adopted the analysis in *Ickes*. *See* 533 F.3d at 1010.[26] But *Ickes* is inapposite because its assumptions have been overtaken by rapid advances in search technologies, the rapidly expanding storage capacity of electronic devices, Am. Compl. ¶ 30, the rise in the number of device searches at the border, *supra* at 3, and the fact that all of the relevant policies explicitly permit suspicionless border searches of devices. The existing regime allows the government to obtain through device searches a quantity and quality of information that imposes a substantial burden on First Amendment rights without justification. Requiring a warrant is necessary to cure this constitutional defect.

CONCLUSION

For the foregoing reasons, Plaintiffs request that this Court deny the Motion to Dismiss.

Respectfully submitted: Dated: January 26, 2018

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

[26] Both *Ickes* and *Arnold* cite to *P.J. Video* in support of their holdings. But *P.J. Video* reaffirms the principle that a warrant requirement can address the First Amendment concerns raised by searches of expressive material, *see* 475 U.S at 877–78—a concern that exists in no less measure when the materials are searched at the border than in the interior of the country.

CERTIFICATE OF SERVICE

I certify that on January 26, 2018, 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