

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

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

Plaintiffs, )

v. )

KEVIN K. MCALEENAN, ACTING )  
SECRETARY OF THE DEPARTMENT OF )  
HOMELAND SECURITY, IN HIS )  
OFFICIAL CAPACITY; JOHN P. )  
SANDERS, CHIEF OPERATING OFFICER )  
AND SENIOR OFFICIAL PERFORMING )  
THE FUNCTIONS AND DUTIES OF THE )  
COMMISSIONER OF U.S. CUSTOMS )  
AND BORDER PROTECTION, IN HIS )  
OFFICIAL CAPACITY; AND MARK A. )  
MORGAN, 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

**MEMORANDUM IN SUPPORT OF DEFENDANTS' CROSS-MOTION FOR  
SUMMARY JUDGMENT AND IN OPPOSITION TO PLAINTIFFS' MOTION FOR  
SUMMARY JUDGMENT**

**TABLE OF CONTENTS**

INTRODUCTION ..... 1

SUMMARY OF UNDISPUTED MATERIAL FACTS..... 2

STANDARD OF REVIEW ..... 6

ARGUMENT ..... 6

I. The Fourth Amendment Does Not Require a Warrant for Border Searches of Electronic Devices ..... 6

    A. The International Border is a Unique Environment Under the Constitution ..... 6

    B. No Court Has Required a Warrant for a Border Search ..... 7

    C. *Riley* Does Not Import a Warrant Requirement into the Border Context..... 8

    D. Plaintiffs’ Facial Challenge is Fatally Overbroad..... 10

    E. The Balance of the Interests Establishes that a Warrant Requirement is Improper..... 12

        i. The Border Search Exemption Serves the Compelling Interests of National Security and Territorial Integrity ..... 12

        ii. Border Searches of Electronic Devices Advance Government Interests in Stopping Contraband..... 13

        iii. The Government has a Significant Interest in Finding Evidence of Violations of Federal Law, an Interest Advanced by Device Searches at the Border ..... 15

        iv. A Warrant Requirement Would Pose a Significant Threat to National Security and Territorial Integrity ..... 17

        v. International Travelers Have a Significantly Reduced Expectation of Privacy ..... 18

        vi. Plaintiffs’ Cursory Alternative Argument for a Lesser Standard Fails..... 20

II. Probable Cause is Not Required to Detain an Electronic Device Anytime a Traveler Leaves the Border..... 22

III. Border Searches of Electronic Devices Do Not Violate the First Amendment..... 23

- A. Expressive Materials Receive No Special Protection from Otherwise Lawful Searches and Seizures ..... 23
- B. A First Amendment Exception at the Border Would Be Unprecedented and Unworkable ..... 25
- IV. Plaintiffs Cannot Establish Standing ..... 26
  - A. Plaintiffs Lack Standing Based on the Likelihood of a Future Search ..... 26
  - B. Plaintiffs Lack Standing to Seek Expungement..... 29
- CONCLUSION..... 30

**TABLE OF AUTHORITIES**

**CASES**

*Abidor v. Napolitano*,  
990 F. Supp. 2d 260 (E.D.N.Y. 2013) ..... 20

*Agostini v. Felton*,  
521 U.S. 203 (1997)..... 9

*Amazon.com LLC v. Lay*,  
758 F. Supp. 2d 1154 (W.D. Wash. 2010)..... 24

*Anderson v. Liberty Lobby, Inc.*,  
477 U.S. 242 (1986)..... 6

*Arizona v. Gant*,  
556 U.S. 332 (2009)..... 19

*Blum v. Holder*,  
744 F.3d 790 (1st Cir. 2014)..... 27

*Buckley v. Valeo*,  
424 U.S. 1 (1976)..... 25

*Chimel v. California*,  
395 U.S. 752 (1969)..... 19

*City of Los Angeles, Calif. v. Patel*,  
135 S. Ct. 2443 (2015)..... 10

*Clapper v. Amnesty Int’l*,  
568 U.S. 398 (2013)..... 26

*Conservation Law Found. v. Pub. Serv. Co. of N.H.*,  
No. 11-CV-353-JL, 2012 WL 4477669 (D.N.H. Sept. 27, 2012) ..... 28

*DeGregory v. Attorney General of New Hampshire*,  
383 U.S. 825 (1966)..... 24

*Gowadia v. United States*,  
Civ. No. 14-00481 SOM/KSC, 2015 WL 5838471 (D. Haw. Oct. 5, 2015)..... 14

*Huongsten Prod. Imp. & Exp. Co. v. Sanco Metals LLC*,  
Civ. No. 10-1610 SEC, 2012 WL 2571301 (D.P.R. July 2, 2012)..... 21

*In re Boucher*,  
No. 2:06-MJ-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009)..... 14

*In re Diaz Cruz*,  
 Br. No. 10-11393 ESL, 2013 WL 3153993 (Bankr. D.P.R. June 19, 2013) ..... 21

*In re Stolar*,  
 401 U.S. 23 (1971)..... 24

*Katz v. Pershing, LLC*,  
 672 F.3d 64 (1st Cir. 2012)..... 30

*Kerin v. Titeflex Corp.*,  
 770 F.3d 978 (1st Cir. 2014)..... 28

*Kissinger v. Reporters Comm. for Freedom of the Press*,  
 445 U.S. 136 (1980)..... 30

*Laird v. Tatum*,  
 408 U.S. 1, (1972)..... 29

*Lamont v. Postmaster Gen. of the U.S.*,  
 381 U.S. 301 (1965)..... 24

*Libertad v. Welch*,  
 53 F.3d 428 (1st Cir. 1995)..... 27

*Luis v. United States*,  
 136 S. Ct. 1083 (2016)..... 25

*Lujan v. Defs. of Wildlife*,  
 504 U.S. 555 (1992)..... 26

*Maine People’s All. And Nat. Res. Def. Council v. Mallinckrodt, Inc.*,  
 471 F.3d 277 (1st Cir. 2006)..... 28

*McIntyre v. Ohio Elections Comm’n*,  
 514 U.S. 334 (1995)..... 26

*New York v. Ferber*,  
 458 U.S. 747 (1982)..... 15

*New York v. P.J. Video, Inc.*,  
 475 U.S. 868 (1986)..... 24

*Osborne v. Ohio*,  
 495 U.S. 103 (1990)..... 15

*Pa. Bd. of Prob. & Parole v. Scott*,  
 524 U.S. 357 (1998)..... 30

*People v. Endacott*,  
164 Cal. App. 4th 1346 (2008) ..... 14

*Reporters Comm. for Freedom of the Press v. Am. Tel. & Tel. Co.*,  
593 F.2d 1030 (D.C. Cir. 1978) ..... 24

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

*Rios v. Dep’t of Educ. of Puerto Rico*,  
Civ. No. 10-1143 ADC/SCC, 2011 WL 7473276 n.1 (D.P.R. Nov. 21, 2011)..... 21

*Rocafort v. IBM Corp.*,  
334 F.3d 115 (1st Cir. 2003)..... 21

*Scott v. United States*,  
436 U.S. 128 (1978)..... 17

*Susan B. Anthony List v. Driehaus*,  
573 U.S. 149 (2014)..... 26

*Turner Broad. Sys. Inc. v. FCC*,  
512 U.S. 622 (1994)..... 25

*United States v. Aleman-Figueroa*,  
117 F. App’x 208 (3d Cir. 2004) ..... 19

*United States v. Alfaro-Moncada*,  
607 F.3d 720 (11th Cir. 2010) ..... 19

*United States v. Arnold*,  
533 F.3d 1003 (9th Cir. 2008) ..... 14, 25

*United States v. Blue*,  
No. 1-14-CR-244-SCJ, 2015 WL 1519159 (N.D. Ga. Apr. 1, 2015)..... 14

*United States v. Boumelhem*,  
339 F.3d 414 (6th Cir. 2003) ..... 7, 19

*United States v. Braks*,  
842 F.2d 509 (1st Cir. 1988)..... 7, 8, 9, 21

*United States v. Brunette*,  
256 F.3d 14 (1st Cir. 2001)..... 24

*United States v. Bunty*,  
617 F. Supp. 2d 359 (E.D. Pa. 2008) ..... 14

*United States v. Caballero*,  
178 F. Supp. 3d 1008 (S.D. Cal. 2016)..... 11, 14

*United States v. Cano*,  
222 F. Supp. 3d 876 (S.D. Cal. 2016)..... 14

*United States v. Chadwick*,  
433 U.S. 1 (1977)..... 19

*United States v. Cotterman*,  
709 F.3d 952 (9th Cir. 2013) ..... 9, 11, 14, 18

*United States v. Cybulski*,  
No. 1:08-CR-8, 2009 WL 3734052 (D. Vt. Oct. 29, 2009) ..... 7

*United States v. Escarcega*,  
685 F. App'x 354 (5th Cir. 2017) ..... 13

*United States v. Feiten*,  
No. 15-20631, 2016 WL 894452 (E.D. Mich. Mar. 9, 2016) ..... 14, 15, 23

*United States v. Flores-Montano*,  
541 U.S. 149 (2004)..... 7, 13, 19, 25

*United States v. Furukawa*,  
No. CRIM 06-145 DSD/AJB, 2006 WL 3330726 (D. Minn. Nov. 16, 2006)..... 14

*United States v. Gonzalez*,  
658 F. App'x 867 (9th Cir. 2016) ..... 14

*United States v. Gurr*,  
471 F.3d 144 (D.C. Cir. 2006)..... 16, 17

*United States v. Hampe*,  
No. CR. 07-3-B-W, 2007 WL 1192365 (D. Me. Apr. 18, 2007) ..... 14

*United States v. Hassanshahi*,  
75 F. Supp. 3d 101 (D.D.C. 2014) ..... 14

*United States v. Hilliard*,  
289 F. App'x 239 (9th Cir. 2008) ..... 14, 25

*United States v. Ickes*,  
393 F.3d 501 (4th Cir. 2005) ..... 14, 25, 26

*United States v. Kapordelis*,  
569 F.3d 1291 (11th Cir. 2009) ..... 14

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

*United States v. Laich*,  
No. 08-20089, 2010 WL 259041 (E.D. Mich. Jan. 20, 2010) ..... 14

*United States v. Levy*,  
803 F.3d 120 (2d Cir. 2015)..... 16, 17

*United States v. Linarez-Delgado*,  
259 F. App'x 506 (3d Cir. 2007)..... 14

*United States v. McAuley*,  
563 F. Supp. 2d 672 (W.D. Tex. 2008)..... 14

*United States v. Mendez*,  
240 F. Supp. 3d 1005 (D. Ariz. 2017) ..... 14

*United States v. Miller*,  
34 F. Supp. 3d 695 (E.D. Mich. 2014)..... 11

*United States v. Molina-Gomez*,  
781 F.3d 13 (1st Cir. 2015)..... 11, 14, 22

*United States v. Molina-Isidoro*,  
884 F.3d 287 (5th Cir. 2018) ..... 9, 13, 22

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

*United States v. Pickett*,  
No. CRIM.A. 07-0374, 2008 WL 4330247 (E.D. La. Sept. 16, 2008)..... 14

*United States v. Ramos*,  
190 F. Supp. 3d 992 (S.D. Cal. 2016)..... 14

*United States v. Saboonchi*,  
990 F. Supp. 2d 536 (D. Md. 2014) ..... 14

*United States v. Sayer*,  
748 F.3d 425 (1st Cir. 2014)..... 25

*United States v. Schoor*,  
597 F.2d 1303 (9th Cir. 1979) ..... 17

*United States v. Scott*,  
334 F. App'x 94 (9th Cir. 2009) ..... 14



*United States v. Seljan*,  
547 F.3d 993 (9th Cir. 2008) ..... 25, 26

*United States v. Singh*,  
295 F. App’x 190 (9th Cir. 2008) ..... 14

*United States v. Stewart*,  
729 F.3d 517 (6th Cir. 2013) ..... 23

*United States v. Touset*,  
890 F.3d 1227 (11th Cir. 2018) ..... *passim*

*United States v. Vergara*,  
884 F.3d 1309 (11th Cir. 2018) ..... 13

*United States v. Verma*,  
No. CRIMA H-08-699-1, 2010 WL 1427261 (S.D. Tex. Apr. 8, 2010) ..... 14

*United States v. Wanjiku*,  
919 F.3d 472 (7th Cir. 2019) ..... 8, 10, 13

*Warden, Md. Penitentiary v. Hayden*,  
387 U.S. 294 (1967) ..... 15, 16

**STATUTES**

6 U.S.C. § 202 ..... 2

6 U.S.C. § 211 ..... 2, 12

31 U.S.C. § 5317 ..... 16

44 U.S.C. § 3314 ..... 30

**RULES**

Fed. R. Civ. P. 56 ..... 6

**REGULATIONS**

19 C.F.R. 161.2 ..... 16

**OTHER AUTHORITIES**

Cyberspace, General Searches, and Digital Contraband,  
105 Yale L.J 1093 (1996) ..... 13

Office of the Privacy Commissioner of Canada, Your Privacy at Airports and Borders,  
<https://www.priv.gc.ca/en/privacy-topics/public-safety-and-law-enforcement/your-privacy-at-airports-and-borders/#toc1a>..... 20

## INTRODUCTION

Every day, well over a million people cross the border of the United States. Over the course of a year, this means over 400 million international travelers. For context, this number is significantly *more* than if every person currently alive in the United States crossed the border in a single year. Additionally, millions of tons of cargo, worth hundreds of billions of dollars, also enter the country each year. Defendants U.S. Customs and Border Protection (“CBP”) and U.S. Immigration and Customs Enforcement (“ICE”), components of Defendant U.S. Department of Homeland Security, are entrusted with monitoring and processing this unceasing, enormous movement of people and goods across our borders.

Given the Government’s paramount interests in national security and the facilitation of lawful trade and travel, officials have been empowered since the founding of the Republic to search all persons and effects at the international border. Unlike searches in the interior of the country, no court has required probable cause or a warrant to conduct a border search. Indeed, the broad border search authority is essential to the Government’s ability to assess and control the vast flow of persons and property across the border; and, to uncover threats to national security, illegal goods and contraband, and evidence of transnational crimes (including export control violations and trafficking in persons or things).

Plaintiffs seek an end to this centuries-old authority. They ask this Court to create an unprecedented rule, a warrant requirement for all searches of electronic devices at the border. This claim lacks any support in law and fact. The Supreme Court has never required probable cause or a warrant in the border search context, and has only once imposed a requirement of reasonable suspicion, in a case involving the prolonged detention of a person suspected of smuggling drugs in her body. *See United States v. Montoya de Hernandez*, 473 U.S. 531, 534-36 (1985). And the Court has declined to hold that the search of a person’s property requires even

that level of suspicion. Contrary to Plaintiffs' assertions, *Riley v. California*, 573 U.S. 373 (2014), which held only that the search of a cell phone incident to arrest requires a warrant, did not *sub silentio* overrule centuries of practice and precedent regarding the breadth of the Government's border search authority. In the multitude of decisions addressing electronic device searches at the border, no court, either before or after *Riley*, has ever held that a warrant is required in the border context. The lack of any applicable precedent in Plaintiffs' favor is not surprising; the Government's paramount interests in national security and territorial integrity at the border outweigh the significantly diminished privacy concerns of travelers. A ruling to the contrary by this Court would push the security of this country into uncharted waters. The Government's ability to know who and what are crossing its borders would be meaningfully undermined; criminals and smugglers would know that they need only carry information in electronic form for it to be protected from search at the border.

This Court should reject Plaintiffs' facial challenges under the First and Fourth Amendments and grant summary judgment for Defendants.

#### **SUMMARY OF UNDISPUTED MATERIAL FACTS**

Congress gave Defendant, Department of Homeland Security ("DHS"), through its components CBP and ICE, broad powers to prevent the entry of terrorists, and the instruments of terrorism into the United States and to enforce numerous criminal and civil federal laws at the border. *See* 6 U.S.C. § 202 (defining DHS responsibilities), § 211 (defining CBP mission responsibilities). Numerous federal statutes and regulations authorize CBP and ICE to inspect and examine all individuals and merchandise entering or departing from the United States, including all types of personal property. *See, e.g.*, 8 U.S.C. §§ 1225, 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a; 22 C.F.R. § 127.4; 19 C.F.R. § 162.6. As the

nation's law enforcement agencies at the border, CBP interdicts, and ICE investigates, a wide range of illegal activities at the border, including but not limited to, child pornography possession and distribution, human rights violations, drug smuggling, weapons trafficking, financial and trade-related crimes, immigration violations, customs requirements, as well as laws relating to national security and terrorism. *See* Declaration of Randy J. Howe ("Howe Decl.") ¶ 7 (Ex. A); Declaration of David L. Denton ("Denton Decl.") ¶ 5 (Ex. B); *see also* PIA dated August 25, 2009 ("2009 PIA") at Bates 221-222 (Ex. C). To accomplish their broad mission responsibilities, Defendants may conduct border searches of all persons and things entering or exiting the United States, including electronic devices. Howe Decl. ¶ 7; *see generally* 2009 PIA.

In August 2009, CBP and ICE issued policies on their longstanding authority to search and inspect electronic devices at the international border. *See generally* Border Searches of Electronic Devices, ICE Directive No. 7-6.1 (Aug. 18, 2009) (Ex. D); Border Search of Electronic Devices Containing Information, CBP Directive No. 3340-049, (Aug. 20, 2009) (Ex. E). In January, 2018, CBP revised its Directive. *See* Border Search of Electronic Devices, CBP Directive No. 3340-049A, (Jan 4, 2018) ("2018 CBP Directive") (Ex. F). Specifically, the 2018 CBP Directive, among other things, (1) clarified the scope of CBP border searches of electronic devices and explicitly stated that measures would be taken to avoid accessing information only stored remotely (*e.g.*, on the "cloud"); (2) distinguished between different types of searches (basic and advanced); and (3) applied a heightened standard for advanced searches (reasonable suspicion or national security concern). *See id.* §5.1. The updated CBP Directive defines an "advanced search" as any search in which an officer connects external equipment, through a wired or wireless connection, to an electronic device, not merely to gain access to the device, but to review, copy and/or analyze its contents. *Id.* § 5.1.4. A basic search is any border search that

is not an advanced search. *Id.* § 5.1.3. The updated Directive further clarified that an advanced search should only be conducted where there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP and ICE, or in which there is a national security concern, and requires advanced supervisory approval. *Id.* § 5.1.4. ICE uses the same definitions of basic and advanced searches and only conducts advanced searches when there is reasonable suspicion present. Stipulated Facts ¶¶ 1, 14. (Ex. G); Denton Decl. ¶ 11; HSI Legal Update – Border Search of Electronic Devices, May 11, 2018 at Bates 1266-67. These policies have been carefully crafted to provide the Government, through DHS and its components, with the tools necessary to secure the nation’s border, while simultaneously striving to protect personal privacy. *See* PIA, January 4, 2018 at Bates 0174-0195 (Ex. H). These policies permit CBP Officers and ICE Special Agents to search information contained in electronic devices subject to the guidelines set forth in the policy directives and any other applicable laws. *See* ICE Directive ¶ 6.1; CBP Directive ¶¶ 4, 5. The policies recognize that it is not always possible to complete the search of a traveler’s electronic device while he or she waits at the border. ICE Directive ¶ 6.1; CBP Directive ¶ 5.4. The policies therefore require the searches of detained devices to be completed in a reasonable time given the facts and circumstances of the particular search. ICE Directive ¶ 8.3(1); CBP Directive ¶ 5.4.

CBP’s mission, to inspect all people and things that cross the border, must be balanced with its mission to facilitate the flow of travelers and trade. Howe Decl. ¶ 8. The sheer volume of people and merchandise passing through the border each day means CBP has a limited amount of time to make decisions regarding the people and goods presented for inspection. *Id.* Upon arrival at a port of entry, at the primary point of inspection, CBP Officers inspect travelers’ documentation (e.g., passport, customs declaration), ask questions regarding their travel and

search CBP systems for relevant information.<sup>1</sup> *Id.* ¶ 13. CBP Officers use their extensive training and experience to identify situations that warrant additional scrutiny. *Id.* ¶ 14.

Given the volume of travelers that CBP processes, and in order to ensure efficiency, if an officer determines that additional scrutiny beyond the brief initial encounter is warranted, the traveler will be referred for a continuation of their inspection, known as secondary inspection. *Id.* At secondary, the CBP Officer may run law enforcement queries through TECS and other systems.<sup>2</sup> *Id.* Additionally, depending on the information the officer gathers, the CBP Officer may request the assistance of ICE. *Id.* ¶ 15; Denton Decl. ¶ 12. CBP Officers and/or ICE Special Agents may conduct an inspection of the traveler and his or her personal belongings, including any electronic devices. Howe Decl. ¶ 15; Denton Decl. ¶¶ 6-7. In FY 2017, CBP conducted 30,524 border searches of electronic devices. In the same time period, CBP processed more than 397 million arriving international travelers, and only 0.007% of arriving travelers had their devices searched. Less than 3,500 of those searches were advanced searches. *See* Stipulated Facts 13; Response to Interrog. 6. (Ex. I). In that same year, ICE conducted only 681 advanced searches, and does not track the small number of basic searches it conducts. Stipulated Facts 15.

---

<sup>1</sup> At primary, a CBP Officer may conduct limited queries of information maintained in TECS, which is the principal CBP law enforcement system. Howe Decl. ¶¶ 9, 12. TECS includes biographical information, manifest information transmitted by the carrier where available, queries against lookouts (such as “wants and warrants” and terrorist watchlist information), vehicle information (in the land environment), and information about the traveler’s prior border crossings. *Id.* The information available to an officer at primary does not generally include information relating to past border searches of electronic devices. CBP does not generally receive advance travel information about individuals traveling across land ports of entry. *Id.*

<sup>2</sup> The information available to officers at secondary includes the same types of information available at primary, but may also include additional records relating to prior encounters between the traveler and CBP. Howe Decl. ¶ 13. ICE Special Agents have access to TECS as well as ICE systems of records that may contain information about any prior ICE encounters with the individual searched. Denton Decl ¶ 14.

Defendants' searches of electronic devices at the border have successfully uncovered threats to national security, illegal activities, contraband, and the inadmissibility of people and things. Howe Decl. ¶¶ 27-30; Denton Decl. ¶¶ 16, 24-27.

Out of the eleven Plaintiffs, seven have had their electronic devices searched at the border only once (Plaintiffs Ghassan Alasaad, Allababidi, Bikkannavar, Gach, Shilby, Wright, and Zorri), and four have had their electronic devices searched at the border more than once (Plaintiffs Merchant, Nadia Alasaad, Dupin and Kushkush). *See* Pls. SUMF ¶¶ 120-149 (ECF 90-2). Except for Plaintiff Merchant, none of the Plaintiffs have had their electronic devices searched since August 2017. Plaintiff Merchant did have her electronic device manually searched in September, 2018 but she has travelled internationally at least five times since her most recent search and has not been searched during any of those trips. *See* Ex. J, Merchant Resp. to Interrogs. 1, 4; Merchant Suppl. Resp. to Interrogs 1, 4, 7.

### STANDARD OF REVIEW

Summary judgment is warranted "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). A fact is material if it can affect the substantive outcome of the litigation, and a dispute is genuine if the evidence is such that a reasonable jury could find for the nonmoving party. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986).

### ARGUMENT

#### **I. The Fourth Amendment Does Not Require a Warrant for Border Searches of Electronic Devices**

##### **A. The International Border is a Unique Environment Under the Constitution**

The United States, as a sovereign nation, has the inherent authority to protect its borders and control who and what crosses into and out of its territory. *See United States v. Flores-*



*Montano*, 541 U.S. 149, 153 (2004). Concomitantly, travelers have a lower expectation of privacy at the border. See *United States v. Montoya de Hernandez*, 473 U.S. 531, 539-40 (1985); *Flores-Montano*, 541 U.S. at 154 (“[T]he expectation of privacy is less at the border than it is in the interior.”). As a result, “the Fourth Amendment’s balance of reasonableness is qualitatively different at the international border than in the interior.” *Montoya de Hernandez*, 473 U.S. at 538.

Due to the unique balance of interests at the border, the Government may search the “persons and effects of entrants . . . [at international borders without being] subject to any requirement of reasonable suspicion, probable cause, or warrant.” *Montoya de Hernandez*, 473 U.S. at 538; see also *United States v. Braks*, 842 F.2d 509, 511 (1st Cir. 1988). This well-established standard permits the Government to search without a warrant *all* of a travelers’ effects, even if those effects fill a forty-foot long shipping container, *United States v. Boumelhem*, 339 F.3d 414, 417 (6th Cir. 2003), or a mobile home. See *United States v. Cybulski*, No. 1:08-CR-8, 2009 WL 3734052, at \*2 (D. Vt. Oct. 29, 2009).

#### B. No Court Has Required a Warrant for a Border Search

In the entire history of the border search exception, the Supreme Court has only once required reasonable suspicion in the context of a border search, in a case involving the prolonged detention of a person suspected of smuggling drugs in her “alimentary canal.” *Montoya de Hernandez*, 473 U.S. at 534-36. Following that holding, lower courts found that particularly invasive personal searches, such as strip searches or body cavity searches, may also require reasonable suspicion at the border. To determine whether a given examination qualifies as a so-called “non-routine” border search (which requires reasonable suspicion), courts in the First Circuit examine the “degree of indignity that accompanies a particular search method rather than

of the extensiveness or thoroughness of the search per se.” *Braks*, 842 F.2d at 512 n. 6 (holding search “routine” even where suspect lifted her skirt to permit border search). Given the high threshold required to find a search “non-routine,” the “Supreme Court has never required reasonable suspicion for a search of property at the border, however non-routine and intrusive.” *United States v. Tousef*, 890 F.3d 1227, 1233 (11th Cir. 2018). Indeed, no suspicion at all is required to support a “routine” border search, that is, any search that is “less intrusive than a strip search[.]” *Braks*, 842 F.2d at 512.

Plaintiffs ask this Court to invent a new category of border searches, apart from “routine” and “non-routine” ones – those that require probable cause and a warrant. Yet “no court has ever required a warrant for any border search or seizure[.]” in light of the paramount Government interests at the border. *United States v. Wanjiku*, 919 F.3d 472, 481 (7th Cir. 2019). There is no legal support for Plaintiffs’ claims, and this Court should reject Plaintiffs’ request to require a warrant for a border search for the first time in history.

C. *Riley* Does Not Import a Warrant Requirement into the Border Context

In the face of case law uniformly rejecting their position, Plaintiffs contend that the Supreme Court’s decision in *Riley* worked a sea change in border search law. Though *Riley* said nothing about border searches, Plaintiffs argue that this Court should extend *Riley* and hold that warrants are required to search “travelers’ electronic devices” at the border. Pls.’ Mot. for Summ. J. at 7, ECF No. 90-1 (“Pls.’ MSJ”).

Yet *Riley* limited its holding to the search incident to arrest exception alone. 573 U.S. at 401-02 (ruling that “other case-specific exceptions may still justify a warrantless search of a particular phone”). The Supreme Court has warned that “[i]f a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the

[lower court] should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions.” *Agostini v. Felton*, 521 U.S. 203, 237 (1997). Here, the Supreme Court’s border search decisions in *Montoya de Hernandez* and *Flores-Montano* control, establishing that invasive border searches of a traveler’s body require only reasonable suspicion, a standard which has never been required for property searches. *See also Braks*, 842 F.2d at 514. This Court should apply the precedent on point, and it should reject Plaintiffs’ request to predict that the Supreme Court may one day require warrants for border searches.<sup>3</sup>

Indeed, “not a single court addressing border searches of computers since *Riley* has read it to require a warrant[.]” *United States v. Molina-Isidoro*, 884 F.3d 287, 292 (5th Cir. 2018). There is some disagreement as to whether even reasonable suspicion is required to conduct an advanced border search of certain electronic devices. *Compare United States v. Touset*, 890 F.3d 1227, 1231 (11th Cir. 2018) (holding that no individualized suspicion is required), *with Kolsuz*, 890 F.3d at 137 (concluding that some level of suspicion is required for forensic searches), *and United States v. Cotterman*, 709 F.3d 952, 962 (9th Cir. 2013) (holding that forensic examination of computer requires reasonable suspicion). But Plaintiffs demand a warrant for every search of every electronic device at the border, an argument rejected by all courts to have so considered. At bottom, the precedents of the Supreme Court and the uniform case law of lower courts, both before and after *Riley*, establish that warrants are not required to conduct border device searches.

---

<sup>3</sup> *Riley* itself noted ample precedent for requiring warrants for certain types of searches in the post-arrest context. *See* 573 U.S. at 392 (noting that when “privacy-related concerns are weighty enough” a “search [of an arrestee] may require a warrant,” and such as in searching the house of an arrestee). By contrast, no court has ever held that a warrant is required for a border search, regardless of the privacy concerns present.

#### D. Plaintiffs' Facial Challenge is Fatally Overbroad

Even assuming *arguendo* that a warrant might ever be required based on the facts of a particular border search, Plaintiffs' facial challenge goes much further, asserting that a warrant is required for every search of every electronic device. The Supreme Court has held that facial challenges under the Fourth Amendment are technically permissible, but cautioned that they are "the most difficult [challenges] . . . to mount successfully," because a plaintiff must show that a challenged practice is "unconstitutional in all of its applications." *City of Los Angeles, Calif. v. Patel*, 135 S. Ct. 2443, 2449, 2451 (2015). Thus, Plaintiffs must show that absent a warrant, any border search of any electronic device violates the Constitution.

Plaintiffs fail to provide any basis for such a sweeping ruling. They repeatedly and erroneously cite *Riley* for the proposition that "electronic devices" all present the same privacy concerns.<sup>4</sup> *See, e.g.*, Pls.' MSJ at 9 (arguing that "*Riley* held that electronic devices differ fundamentally . . . from physical containers."). But *Riley* addressed only cell phones, not the entire universe of electronic devices, and portable electronic devices vary widely in terms of purpose, content, and potential privacy concerns. *See, e.g., Wanjiku*, 919 F.3d at 485 n.15 (noting that "[t]o the extent that *Riley* gives heightened protection to cell phone data, it is not at all clear" that such protection could apply to a "micro SD card inserted into the phone"); *United*

---

<sup>4</sup> Plaintiffs fail to clearly define what they mean by those "electronic devices" for which a warrant is required at the border. The most Plaintiffs say in their Amended Complaint is that such devices "include," but are apparently not limited to, "mobile phones, laptops, tablets, digital cameras, and portable digital storage devices." Am. Compl. ¶ 27. Plaintiffs themselves complain that not only were their cellphones and laptops searched at the border, but that Defendants also searched other electronic devices such as digital cameras and an "electronic voice recorder." Am. Compl. ¶ 108. Accordingly, Plaintiffs seek a ruling far broader than that set forth in *Riley*, which concerned only cellphones.

*States v. Miller*, 34 F. Supp. 3d 695, 699 (E.D. Mich. 2014) (explaining that search of a digital camera “does not raise the same privacy concerns as a cell phone”).

Further, not only must Plaintiffs show that a warrant is required to search every type of electronic device at the border, they must also show that every conceivable search of those devices, no matter its duration, similarly requires a warrant. That is, Plaintiffs must establish that even the briefest search, wherein an officer merely verifies that a laptop is operational and contains data, for instance, requires a warrant. *See U.S. v. Molina-Gomez*, 781 F.3d 13, 15 (1st Cir. 2015) (noting that border officers verified a laptop was operational, but saw it contained no data). Likely anticipating an uphill climb, Plaintiffs preemptively argue that “there is no valid distinction between manual and forensic device searches at the border.” Pls.’ MSJ at 28.

Plaintiffs thus urge this Court to rule there is no material difference between a brief manual search of a few minutes or seconds, and a forensic examination involving specialized hardware, where all data, potentially including deleted files, may be copied or analyzed.

Yet the duration and nature of a search are highly relevant factors when considering reasonableness under the Fourth Amendment. *See, e.g., United States v. Caballero*, 178 F. Supp. 3d 1008, 1016 (S.D. Cal. 2016) (finding no reasonable suspicion required for device border search in part because of short duration of search). And while some courts have held that no suspicion is ever required for device border searches, *see Tousef*, 890 F.3d 1227, those courts that have required reasonable suspicion have done so only for certain “forensic” searches, that allow for searching a greater “breadth of private information.” *See, e.g., Kolsuz*, 890 F.3d at 145; *Cotterman*, 709 F.3d 966. In fact, CBP and ICE both require that an agent have reasonable suspicion or a valid national security concern to conduct an advanced search, requirements not mandated for a basic search.

Thus, even if some searches of electronic devices could possibly require heightened suspicion at the border, Plaintiffs have not even attempted to show that a warrant is required for *every* possible border search of *every* electronic device. And because Plaintiffs cannot show that the Constitution is violated anytime an electronic device is searched absent a warrant, their facial claim necessarily fails.

E. The Balance of the Interests Establishes that a Warrant Requirement is Improper

Even if the unbroken line of decisions rejecting warrants at the border and the high bar of Plaintiffs' facial challenge were not enough to reject their claims, an analysis of the relevant interests here compels the same conclusion.

i. The Border Search Exemption Serves the Compelling Interests of National Security and Territorial Integrity

The Court in *Riley* reiterated that searches conducted pursuant to an exception to the warrant requirement are “reasonable regardless of the probability” that contraband or evidence will be discovered in any particular situation. 573 U.S. at 386. The question then is whether warrantless border device searches would entirely “untether the rule from the justifications underlying the . . . [border search] exception.” *See id.*

The Supreme Court has repeatedly recognized the broad justifications of national security and “territorial integrity”<sup>5</sup> underpinning the border search exception. *See, e.g., Flores-Montano,*

---

<sup>5</sup> The terms “territorial integrity” and “integrity of the border,” are used as shorthand here for the numerous specific interests entrusted to Defendants by statute, interests which are advanced by border searches. These interests include, among other things: the responsibility to “ensure the interdiction of persons and goods illegally entering or exiting the United States;” “facilitate and expedite the flow of legitimate travelers and trade;” “administer the . . . enforcement of the customs and trade laws of the United States;” “detect, respond to, and interdict terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States;” and “enforce and administer all immigration laws.” *See* 6 U.S.C. § 211.

541 U.S. at 153, *Montoya de Hernandez*, 473 U.S. at 544 ([C]ustoms officials have *more* than merely an investigative law enforcement role. They are *also* charged . . . with protecting this Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics, or explosives.”) (emphasis added). Accordingly, because an electronic device border search helps to ensure national security; prevent the entry of criminals, inadmissible aliens, and contraband; and otherwise facilitates lawful trade and travel, the purposes of the border search exception are served.

ii. Border Searches of Electronic Devices Advance Government Interests in Stopping Contraband

Even Plaintiffs concede that the detection and interdiction of contraband, Pls.’ MSJ at 12, is a valid basis for suspicionless border searches. And the undisputed evidence shows that that electronic border device searches advance this Government interest. Electronic devices can contain illegal goods just as easily as any other container. There are many types of “digital contraband,” but examples include: child pornography, classified information, stolen credit card numbers, counterfeit media, and programs designed specifically to hack into other computers. *See* Howe Decl. ¶ 23; Denton Decl. ¶ 7; Note: Cyberspace, General Searches, and Digital Contraband, 105 Yale L.J 1093, 1097 (1996). Moreover, electronic devices can contain evidence of contraband, such as in instances of drug trafficking, firearm smuggling, and export control violations. Howe Decl. ¶¶ 23; Denton Decl ¶¶ 8-9, 17, 24-27. In fact, border device searches have uncovered contraband and evidence of illegal goods with regularity.<sup>6</sup>

---

<sup>6</sup> *See, e.g., United States v. Wanjiku*, 919 F.3d 472, 474 (7th Cir. 2019) (child pornography); *United States v. Kolsuz*, 890 F.3d 133, 136 (4th Cir. 2018) (evidence of firearm smuggling); *United States v. Tousez*, 890 F.3d 1227, 1230 (11th Cir. 2018) (child pornography); *United States v. Vergara*, 884 F.3d 1309, 1311 (11th Cir. 2018) (child pornography); *United States v. Molina-Isidoro*, 884 F.3d 287, 289 (5th Cir. 2018) (evidence of drug trafficking); *United States v. Escarcega*, 685 F. App’x 354, 354 (5th Cir. 2017) (evidence of drug trafficking); *United States v.*

Notably, in *Riley*, the Court found that the narrow considerations underlying the search incident to arrest exception, physical danger to officers and the threat of evidence destruction, were either nonexistent or rarely applicable in the context of cell phones. 573 U.S. at 389 (noting “a couple of anecdotal examples” of remote data wiping). Here, there is no reasonable

---

*Gonzalez*, 658 F. App’x 867, 869 (9th Cir. 2016) (evidence of drug trafficking); *United States v. Molina-Gomez*, 781 F.3d 13, 17 (1st Cir. 2015) (evidence of drug trafficking); *United States v. Cotterman*, 709 F.3d 952, 956 (9th Cir. 2013) (child pornography); *United States v. Scott*, 334 F. App’x 94, 95 (9th Cir. 2009) (child pornography); *United States v. Kapordelis*, 569 F.3d 1291 (11th Cir. 2009) (child pornography); *United States v. Arnold*, 533 F.3d 1003, 1005 (9th Cir. 2008) (child pornography); *United States v. Hilliard*, 289 F. App’x 239, 239 (9th Cir. 2008) (child pornography); *United States v. Singh*, 295 F. App’x 190, 191 (9th Cir. 2008) (evidence of immigration fraud and identity theft); *United States v. Linarez-Delgado*, 259 F. App’x 506, 507 (3d Cir. 2007) (evidence of drug trafficking); *United States v. Ickes*, 393 F.3d 501, 502 (4th Cir. 2005) (child pornography); *United States v. Mendez*, 240 F. Supp. 3d 1005, 1007 (D. Ariz. 2017) (evidence of drug trafficking); *United States v. Caballero*, 178 F. Supp. 3d 1008, 1011-12 (S.D. Cal. 2016) (evidence of drug trafficking); *United States v. Cano*, 222 F. Supp. 3d 876, 877-78 (S.D. Cal. 2016) (evidence of drug trafficking); *United States v. Ramos*, 190 F. Supp. 3d 992, 994 (S.D. Cal. 2016) (evidence of drug trafficking); *United States v. Feiten*, No. 15-20631, 2016 WL 894452, at \*1 (E.D. Mich. Mar. 9, 2016) (child pornography); *Gowadia v. United States*, Civ. No. 14-00481 SOM/KSC, 2015 WL 5838471, at \*5 (D. Haw. Oct. 5, 2015) (unlawful export of classified information); *United States v. Blue*, No. 1-14-CR-244-SCJ, 2015 WL 1519159, at \*1 (N.D. Ga. Apr. 1, 2015) (evidence of drug trafficking); *United States v. Hassanshahi*, 75 F. Supp. 3d 101, 104 (D.D.C. 2014) (evidence of violations of trade embargo against Iran); *United States v. Saboonchi*, 990 F. Supp. 2d 536, 539 (D. Md. 2014) (evidence of export violations); *United States v. Verma*, No. CRIMA H-08-699-1, 2010 WL 1427261, at \*2 (S.D. Tex. Apr. 8, 2010) (child pornography); *United States v. Laich*, No. 08-20089, 2010 WL 259041, at \*2 (E.D. Mich. Jan. 20, 2010) (child pornography); *In re Boucher*, No. 2:06-MJ-91, 2009 WL 424718, at \*1 (D. Vt. Feb. 19, 2009) (child pornography); *United States v. Bunty*, 617 F. Supp. 2d 359, 363 (E.D. Pa. 2008) (child pornography); *United States v. McAuley*, 563 F. Supp. 2d 672, 675 (W.D. Tex. 2008) (child pornography); *United States v. Pickett*, No. CRIM.A. 07-0374, 2008 WL 4330247, at \*1 (E.D. La. Sept. 16, 2008) (child pornography); *United States v. Hampe*, No. CR. 07-3-B-W, 2007 WL 1192365, at \*5 (D. Me. Apr. 18, 2007) (child pornography); *United States v. Furukawa*, No. CRIM 06-145 DSD/AJB, 2006 WL 3330726, at \*2 (D. Minn. Nov. 16, 2006) (child pornography); *People v. Endacott*, 164 Cal. App. 4th 1346, 1348 (2008) (child pornography).



dispute that seizures of contraband and evidence of violations of federal law via device border searches, of which there are many examples, materially advance the interests of the Government.

Yet, Plaintiffs assert that the Government has a reduced interest in interdicting electronic contraband such as child pornography at the border, because it is “primarily transported across borders via the internet, not ports of entry.” ECF No. 90-1 at 16. The Government’s interest in seizing contraband at the border, especially something as harmful as child pornography, is not reduced simply because the same or similar contraband might be available elsewhere.<sup>7</sup> As the Supreme Court has held, “[g]iven the importance of the State’s interest in protecting the victims of child pornography, we cannot fault [the government] for attempting to stamp out this vice at all levels in the distribution chain.” *See Osborne v. Ohio*, 495 U.S. 103, 110-11 (1990); *see also New York v. Ferber*, 458 U.S. 747, 757 (1982) (“The prevention of sexual exploitation and abuse of children constitutes a government objective of surpassing importance.”). Border searches of electronic devices thus advance Government interests “by preventing unwanted goods from crossing the border into the country.” *United States v. Feiten*, Case No. 15-20631, 2016 WL 894452, at \*6 (E.D. Mich. Mar. 9, 2016).

iii. The Government has a Significant Interest in Finding Evidence of Violations of Federal Law, an Interest Advanced by Device Searches at the Border

Plaintiffs also argue that the Government has a lesser interest in finding evidence of legal violations, as opposed to contraband itself. Pls.’ MSJ at 13. This distinction has been roundly rejected in the case law. *See Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 309-10 (1967) (rejecting distinction in search warrant context between evidence and contraband). As the Supreme Court ruled, “there is no viable reason to distinguish intrusions to secure ‘mere

---

<sup>7</sup> Applying this reasoning, it would be unreasonable for Defendants to conduct searches for narcotics because they may also be available domestically. Howe Decl. ¶ 40.

evidence’ from intrusions to secure fruits, instrumentalities, or contraband.” *Id.* at 310. The few courts to have considered this argument in the border context agree that any distinction “between contraband and documentary evidence of a crime is without legal basis.” *United States v. Gurr*, 471 F.3d 144, 149 (D.C. Cir. 2006); *see also Kolsuz*, 890 F.3d at 143-44 (upholding border search of phone “to uncover information about an ongoing transnational crime,” as such efforts “fit[] within the core of the rationale underlying the border search exemption”); *United States v. Levy*, 803 F.3d 120, 124 (2d Cir. 2015) (finding that quick review of a notebook at the border is a “routine” search, requiring no suspicion).

Indeed, the need to uncover information is vital to the Government’s interest in safeguarding the border. As the Howe Declaration explains, given the uniqueness of the border, a border officer will often be unable to immediately determine whether a person or their goods are inadmissible, or otherwise violate any laws.<sup>8</sup> Howe Decl. ¶ 19. Border officers can only make such a determination because they are able to gather information concerning the traveler and their effects. *See id.* ¶¶ 22, 26; Denton Decl. ¶¶ 17, 24-27. The Government’s interest in uncovering evidence thus cannot be distinguished from, or diminished in relation to, the corresponding interest in locating contraband itself.

Plaintiffs fare no better with their final argument on this point: that the Government has a lesser interest in enforcing laws that are “not confined to possible violations of immigration and customs laws.” Pls.’ MSJ at 13. But “the important factor for a court to consider is whether the

---

<sup>8</sup> In addition to criminal laws that apply at the border, CBP is responsible for enforcing civil and administrative legal regimes, including the civil and administrative aspects of the nation’s customs and immigration laws. In addition, CBP and ICE enforce a variety of other federal laws applicable at the border, such as those relating to counterterrorism, 6 U.S.C. § 211(g)(3), transnational money laundering, 31 U.S.C. § 5317, economic sanctions, 19 C.F.R. 161.2(a), and import and export controls on arms and implements of war, controlled substances, and radiological material, *id.*

search was conducted under proper authority, not the ‘underlying intent or motivation of the officers involved.’” *See Gurr*, 471 F.3d at 149 (quoting *Scott v. United States*, 436 U.S. 128, 138 (1978)). While neither CBP nor ICE will initiate searches for reasons that lack a nexus to the border, Howe Decl. ¶ 17; Denton Decl. ¶ 10, courts have consistently dismissed objections to border searches because border officers collaborated with other agencies, for instance, or otherwise uncovered items unrelated to customs violations. *See, e.g., Levy*, 803 F.3d at 124 (“Official interagency collaboration, even (and perhaps especially) at the border, is to be commended, not condemned.”); *United States v. Schoor*, 597 F.2d 1303, 1306 (9th Cir. 1979) (Kennedy, J.) (“That the search was made at the request of the DEA officers does not detract from its legitimacy.”).

iv. A Warrant Requirement Would Pose a Significant Threat to National Security and Territorial Integrity

Because border searches of electronic devices advance the Government’s interests, imposing a warrant requirement would necessarily threaten the security of this country. As explained above, Defendants have on numerous occasions interdicted contraband and criminals through device border searches, and in most, if not all, of these instances the Government did not have a warrant or probable cause. *See* Howe Decl. ¶ 33-35; Denton Decl. ¶¶ 23-27. It is highly likely, then, that had such requirements been in place, the vast majority of the criminals cited above would have crossed the border undetected, free to violate federal law.

If Defendants were required to obtain a warrant before performing any electronic border search, they will be unable to do so in the vast majority of cases, given the limited advance information regarding travelers and their possessions that may come across the border on any given day. Howe Decl. ¶¶ 33-34; Denton Decl. ¶ 22. A warrant requirement for electronic devices like cell phones “would create special protection for the property most often used to

store and disseminate child pornography,” and other digital contraband. *Touset*, 890 F.3d at 1235. This safe-haven for electronic devices would also “significantly aid[] technologically savvy terrorists and criminals who rely on encryption and other surreptitious forms of data storage in their efforts to do harm.” *Cotterman*, 709 F.3d at 985 (Smith, J., dissenting). Such a rule would obviate the deterrent effect of border searches for electronic devices and incentivize criminals to store contraband or other evidence of illegal goods on their electronic devices. *See* Howe Decl. ¶¶ 38, 43; Denton Decl. ¶¶ 18, 23-27. Moreover, a warrant requirement would likely impose additional logistical and resource requirements on Defendants. Howe Decl. ¶¶ 36-37; Denton Decl. ¶¶ 19-22.

In light of the real threats to law enforcement and the further unknown effects of requiring *any* level of suspicion for all device border searches, Plaintiffs’ requested judicial relief would create real safety and security risks. Howe Decl. ¶ 35. As one jurist noted in this context, “th[is] whole enterprise calls for the greatest caution and circumspection, not premature declarations of constitutional rules.” *Kolsuz*, 890 F.3d at 148 (Wilkinson, J., concurring). This admonition was echoed by Justice Alito in *Riley*, where he noted that “[l]egislatures, elected by the people, are in a better position than [courts] are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.” 573 U.S. at 408 (Alito, J. concurring). The significant risks posed by a warrant requirement at the border weigh strongly against Plaintiffs’ claims.

v. International Travelers Have a Significantly Reduced Expectation of Privacy

In contrast to the Government’s vital interests and heightened authority, travelers maintain only a diminished expectation of privacy at the international border. “[O]n many occasions, [the Supreme Court has] noted that the expectation of privacy is less at the border

than it is in the interior.” *Flores-Montano*, 541 U.S. at 154. Plaintiffs reason that even though arrestees also have “diminished privacy interests,” Pls.’ MSJ at 10, a warrant was still required to search their cell phones in *Riley*.

But a traveler’s expectation of privacy at the international border differs from that of an arrestee. Even in a search incident to arrest, the search of an arrestee’s home, luggage, or vehicle generally requires a warrant. *See Arizona v. Gant*, 556 U.S. 332, 351 (2009) (requiring warrant to search vehicle incident to arrest, excepting certain circumstances); *United States v. Chadwick*, 433 U.S. 1, 11 (1977) (requiring warrant to search locked footlocker incident to arrest); *Chimel v. California*, 395 U.S. 752, 762 (1969) (requiring warrant for search of home incident to arrest). All such similar searches at the border are conducted without a warrant, and in many instances not even reasonable suspicion is required. *See, e.g., Flores-Montano*, 541 U.S. 149 (upholding border search of vehicle absent reasonable suspicion); *United States v. Alfaro-Moncada*, 607 F.3d 720, 728 (11th Cir. 2010) (upholding suspicionless border search of ship cabin, which served as a “crew member’s home”); *United States v. Aleman-Figueroa*, 117 F. App’x 208, 212 (3d Cir. 2004) (upholding warrantless border search of ship cabin and locked safe therein). Travelers are thus on notice that they may be searched at the border without probable cause or a warrant; the same for their effects, whether contained in a locked suitcase, their vehicle, or even their home.

In addition, a traveler’s expectation of privacy is lessened even further at the border because, by definition, he or she is traveling to a foreign country, outside the jurisdiction of the Fourth Amendment. *See Boumelhem*, 339 F.3d at 423 (explaining that travelers have “a lesser expectation of privacy when they (or their goods) leave the country [because they will enter] . . . another country which will likely conduct its own border search”); *Abidor v. Napolitano*, 990 F.

Supp. 2d 260, 277 (E.D.N.Y. 2013) (holding that travelers cannot reasonably expect their devices “will be immune from searches” in foreign countries).<sup>9</sup> Plaintiffs cannot reasonably expect that their electronic devices will be immune from search in the countries they visit.

Thus, whatever subjective privacy interests travelers might have in their electronic devices, any *reasonable* expectation of privacy is significantly reduced in the border context. And “not only is the expectation of privacy less at the border than in the interior, the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border.” *Montoya de Hernandez*, 473 U.S. at 539-40. Plaintiffs thus cannot establish that a warrant is required to conduct a border device search, let alone all border device searches.

vi. Plaintiffs’ Cursory Alternative Argument for a Lesser Standard Fails

Plaintiffs spend two brief paragraphs urging that even if this Court holds that no warrant is required, it should still demand some “heightened standard of suspicion” for device border searches. Pls’ MSJ at 19-20. Plaintiffs first argue that probable cause should still be mandated, even in the absence of a warrant requirement, for the sole reason that it is “necessary” to cabin the “privacy intrusion of such searches.” *Id.* While this Court should not consider such a “vague and undeveloped argument,” a blanket probable cause standard is just as unprecedented at the border as a warrant requirement, and Plaintiffs’ assertion should be rejected for the reasons set

---

<sup>9</sup> For instance, the Canadian Government has published a policy stating that their officials may search “personal devices” at the Canadian border if there are “grounds or indications that ‘evidence of contraventions may be found on the digital device or media.’” *See* Office of the Privacy Commissioner of Canada, *Your Privacy at Airports and Borders*, <https://www.priv.gc.ca/en/privacy-topics/public-safety-and-law-enforcement/your-privacy-at-airports-and-borders/#toc1a>.

forth above. *See Rios v. Dep't of Educ. of Puerto Rico*, Civ. No. 10-1143 ADC/SCC, 2011 WL 7473276, at \*1 n.1 (D.P.R. Nov. 21, 2011).

The same result is true for Plaintiffs' equally brief and belated invocation of the reasonable suspicion standard. In a three-sentence mention of reasonable suspicion, Plaintiffs fail to clearly state whether they are asking this Court to require reasonable suspicion for all device searches. *See* Pls.' MSJ at 20. As a result, their "failure to proffer a developed argument [on these] contentions is tantamount to waiver." *See Huongsten Prod. Imp. & Exp. Co. v. Sanco Metals LLC*, Civ. No. 10-1610 SEC, 2012 WL 2571301, at \*4 (D.P.R. July 2, 2012); *see also Rocafort v. IBM Corp.*, 334 F.3d 115, 121 (1st Cir. 2003) ("[P]assing reference to legal phrases and case citation without developed argument is not sufficient to defeat waiver."). Moreover, Plaintiffs' Amended Complaint states only that the Constitution is violated by device border searches "absent a warrant supported by probable cause." Am. Compl. at 39-42. Plaintiffs have not sought to further amend their Complaint to add a "reasonable suspicion" claim, and cannot do so through their Motion for Summary Judgment. *See In re Diaz Cruz*, Br. No. 10-11393 ESL, 2013 WL 3153993, at \*6 (Bankr. D.P.R. June 19, 2013) (collecting cases holding that "a party cannot seek summary judgment for himself on a new claim that has not been pled in his complaint."). The parties have proceeded in this case on the claims articulated in the operative Complaint; Plaintiffs should not be heard to argue otherwise.

To the extent the Court considers this argument at all, it should be rejected. Plaintiffs cannot establish that *every* border search of *every* electronic device is just as "intrusive" as a "strip search," as required to demand reasonable suspicion in the First Circuit. *Braks*, 842 F.2d at 514. Indeed, no court has held that all device border searches require reasonable suspicion.

*See Molina-Isidoro*, 884 F.3d at 293. Just as a warrant is not required for every device border search, reasonable suspicion is also not mandated by the Constitution for device searches.

## **II. Probable Cause is Not Required to Detain an Electronic Device Anytime a Traveler Leaves the Border**

Plaintiffs next argue that the Government must have probable cause to detain “electronic devices after a traveler has left the border.” Pls.’ MSJ at 22. But this facial challenge is foreclosed by the First Circuit’s decision in *Molina-Gomez*. There, CBP detained and searched the defendant’s laptop and PlayStation for 22 days after the defendant left the border and “had been allowed entry into the United States.” *Molina-Gomez*, 781 F.3d at 21 n. 4. The First Circuit held that this border search was either “routine,” requiring no individualized suspicion, or “non-routine,” requiring reasonable suspicion. *Id.* at 19. But the Court ultimately held that it need not decide this question, because CBP had reasonable suspicion justifying their search. *Id.* at 19-20. Further, the First Circuit held that the search was not rendered unreasonable “during the twenty-two days the electronics were detained.” *Id.* at 21. Thus, binding First Circuit precedent establishes that, at most, reasonable suspicion is required to detain an electronic device past the time a traveler leaves the border. Plaintiffs’ argument to require probable cause should be rejected for this reason alone.

Even if *Molina-Gomez* did not doom Plaintiffs’ argument, it would remain foreclosed by Supreme Court precedent. Indeed, the Supreme Court has “consistently rejected hard-and-fast time limits” for searches and detentions, including those at the border. *Montoya de Hernandez*, 473 U.S. at 543. Yet, contrary to the Supreme Court’s teachings, a hard-and-fast time limit is precisely what Plaintiffs seek here. *See* Pls.’ MSJ at 22.<sup>10</sup> Under Plaintiffs’ argument, the

---

<sup>10</sup> Plaintiffs fail raise any substantive argument as to why Defendants’ policies are unreasonable in terms of how long devices may be detained, nor do Plaintiffs specify what time limits or other



moment a traveler leaves the border, Defendants must have probable cause to detain the traveler's electronic device.

Such a framework would foreclose any consideration of the relevant facts and circumstances of a given border search, including whether the Government was unable to conduct a border search of a device immediately because of a lack of proper equipment, *United States v. Stewart*, 729 F.3d 517, 526 (6th Cir. 2013), difficulty with software, *Feiten*, 2016 WL 894452 at \*1, or password-protected files. The Supreme Court in *Montoya de Hernandez* held that a court must consider all relevant circumstances when evaluating the duration of a detention at the border. 473 U.S. at 543. Plaintiffs can thus muster no support for the arbitrary and inflexible time limit they seek, and their claim should accordingly be rejected.

### **III. Border Searches of Electronic Devices Do Not Violate the First Amendment**

#### **A. Expressive Materials Receive No Special Protection from Otherwise Lawful Searches and Seizures**

Plaintiffs' final, brief claim is that warrantless border searches also violate the First Amendment, because such searches cover "personal . . . communications and associations." Pls.' MSJ at 23. As this Court recognized, "Plaintiffs' Fourth and First Amendment claims are closely related." Mem. & Order, at 52 n. 15, ECF No. 34 ("Order"). Indeed, it would be incongruous to find that warrantless border searches are reasonable under the Fourth Amendment, but unreasonable under First Amendment. And for good reason, the Supreme Court has held that the First Amendment does not shield so-called expressive materials from otherwise lawful searches under the Fourth Amendment. *See New York v. P.J. Video, Inc.*, 475

---

guidance is required by the Fourth Amendment. Accordingly, Defendants read this ground of Plaintiffs' Motion for Summary Judgment as limited to argument that "[a]bsent probable cause, confiscations of electronic devices after a traveler has left the border violate the Fourth Amendment." Pls.' MSJ at 22.

U.S. 868, 875 (1986) (rejecting “any suggestion that the standard of probable cause in the First Amendment area is different than in other contexts”); *United States v. Brunette*, 256 F.3d 14, 17 (1st Cir. 2001) (concluding that the Fourth Amendment analysis “is no different where First Amendment concerns may be at issue”).

Nor do “persons engaging in certain types of First Amendment activity have broader Fourth Amendment rights than other citizens.” *Reporters Comm. for Freedom of the Press v. Am. Tel. & Tel. Co.*, 593 F.2d 1030, 1055 (D.C. Cir. 1978). Thus, “the existence of First Amendment ‘interests’ does not give rise to any substantive or procedural protections above and beyond those afforded by the Fourth Amendment.” *Id.* at 1056. Because expressive materials do not receive heightened protection from search and seizure, the Fourth Amendment inquiry here alone governs. *Id.* at 1055. Since warrantless border searches of electronic devices pass muster under the Fourth Amendment, the same result is appropriate in the First Amendment context as well.

Even if Plaintiffs’ First Amendment claim could have some independent force, it fails for the simple reason that Defendants’ policies do not target speech or expression at all.<sup>11</sup> Border searches are not aimed at uncovering protected, expressive materials, but rather at contraband or evidence of the violation of federal laws enforced at the border. Thus, the policies can have only an incidental burden, if any, on First Amendment rights. *Cf. United States v. Sayer*, 748 F.3d

---

<sup>11</sup> Plaintiffs’ cited cases are inapposite. All involve instances of compelled disclosure, involving the targeting of specific First Amendment-protected materials. *See, e.g., In re Stolar*, 401 U.S. 23 (1971) (disclosure of bar applicant’s organizational membership); *DeGregory v. Attorney General of New Hampshire* 383 U.S. 825 (1966) (investigation by state attorney general regarding involvement in communist activities); *Lamont v. Postmaster Gen. of the U.S.*, 381 U.S. 301, 302 (1965) (detention of mail that the Post Office labeled “communist political propaganda”); *Amazon.com LLC v. Lay*, 758 F. Supp. 2d 1154, 1167–70 (W.D. Wash. 2010) (disclosure of information related to online retailer’s sales, including consumer names and purchase information).

425, 433-34 (1st Cir. 2014) (“Speech integral to criminal conduct is . . . a ‘long-established category of unprotected speech.’”). And Supreme Court “precedents hold that a generally applicable law placing only an incidental burden on a constitutional right does not violate that right.” *Luis v. United States*, 136 S. Ct. 1083, 1101-02 (2016).

The same result would obtain even assuming, *arguendo*, that the policies had more than an incidental burden on speech. As this Court has pointed out, CBP and ICE policies are content-neutral. Order at 48. Therefore the policies are not, as Plaintiffs claim, subject to strict scrutiny. *See Turner Broad. Sys. Inc. v. FCC*, 512 U.S. 622 (1994) (describing the strict scrutiny reserved for content-based restrictions of speech). Thus, to the extent that this Court requires a “substantial relation,” *Buckley v. Valeo*, 424 U.S. 1, 64 (1976), between the governmental interest and information sought in a border search, that standard is clearly met. Border searches of electronic devices are directed at preventing the entry of inadmissible persons and things, and interdicting threats to border security. The Government’s interest in uncovering such malfeasance is “paramount” at the border, and device searches are clearly related to that interest. *See Flores-Montano*, 541 U.S. at 149.

B. A First Amendment Exception at the Border Would Be Unprecedented and Unworkable

Plaintiffs’ attempt to create a First Amendment exception to the well-established border search doctrine has no support in precedent and would cause enormous practical problems at the border. The courts that have entertained this argument have specifically rejected it, holding that there is no First Amendment exception to the border search doctrine. *Ickes*, 393 F.3d at 507; *Arnold*, 533 F.3d at 1010; *United States v. Seljan*, 547 F.3d 993, 1011-12 (9th Cir. 2008) (Callahan, J., concurring); *Hilliard*, 289 F. App’x at 239-40.

Indeed, it is hard to fathom why data on an electronic device should command greater respect from the First Amendment than physical pamphlets or art. *Cf. McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 346 (1995) (holding that distribution of political leaflets “occupies the core of the protection afforded by the First Amendment”). Plaintiffs’ argument, if accepted, raises troubling questions as to whether *any* expressive material could be subject to a border search, thereby forcing officers “to engage in the sort of decision-making process that the Supreme Court wishes to avoid in sanctioning expansive border searches.” *Seljan*, 547 F.3d at 1011 (Callahan, J., concurring). Creating such a broad and impractical exception would have “staggering” consequences. *See Ickes*, 393 F.3d at 506. At bottom there is no basis for a First Amendment exception to the well-established border search doctrine.

#### **IV. Plaintiffs Cannot Establish Standing**

This Court previously found that Plaintiffs plausibly alleged standing at the pleading stage, on the same general arguments that Plaintiffs re-raise in their Motion for Summary Judgment. The Government maintains its position that Plaintiffs lack standing to pursue their claims.

##### **A. Plaintiffs Lack Standing Based on the Likelihood of a Future Search**

To establish standing, Plaintiffs must show: (1) an injury in fact; (2) a causal connection between the injury and the challenged conduct of the defendant; and (3) a likelihood that a favorable ruling will redress the alleged injury. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992). “An allegation of future injury may suffice if the threatened injury is ‘certainly impending,’ or there is a ‘substantial risk’ that the harm will occur.” *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper v. Amnesty Int’l*, 568 U.S. 398, 414 n.5 (2013)). “To establish these elements of standing at the summary judgment stage of a

proceeding, a plaintiff cannot rest on mere allegations, but must set forth by affidavit or other evidence specific facts[.]” *Libertad v. Welch*, 53 F.3d 428, 436 (1st Cir. 1995).

Plaintiffs claim standing on the basis that they will be “exposed” to Defendants’ policies on border searches in the future, and therefore suffer “probabilistic injury.” Pls.’ MSJ at 27; *but see Blum v. Holder*, 744 F.3d 790, 797 n.9 (1st Cir. 2014) (noting that the Supreme Court has “signaled a renewed caution about finding injury in fact based on probabilistic injury”). In assessing this argument, individual Plaintiffs can be broken down into two categories: (1) those who have been searched multiple times at the border (Plaintiffs Merchant, Nadia Alasaad, Dupin and Kushkush), and (2) those who have been searched only once (Plaintiffs Ghassan Alasaad, Allababidi, Bikkannavar, Gach, Shilby, Wright, and Zorri).<sup>12</sup>

With regard to the seven plaintiffs who have been searched only once at the border, these Plaintiffs do not establish that they are at any greater risk of a future device search than the other millions of Americans who travel internationally every year. Their argument is that a 0.007% chance of a border device search, the stipulated frequency of such searches of arriving travelers, suffices for a “substantial risk” of injury.<sup>13</sup> *See Maine People’s All. And Nat. Res. Def. Council*

---

<sup>12</sup> Defendants do not address here the specific circumstances of each Plaintiff’s device search or detention, as these facts are not material to Plaintiffs’ facial legal challenges or their assertions of standing. *See* Joint Stmt & Proposed Discovery Schedule, at 4, ECF No. 58 (Plaintiffs agreed that “[t]his Court need not address . . . any factual predicate for Defendants’ past searches and confiscations of Plaintiffs’ electronic devices at the border”). In addition, such facts may touch on law enforcement sensitive issues such as the procedures followed and the bases for specific searches and detentions. To the extent that this Court concludes that such issues are relevant to this motion, Defendants would be willing provide the Court with any official records that may exist, on an *ex parte* and *in camera* basis.

<sup>13</sup> Plaintiffs briefly argue, in a bullet, that because border officers “may” access records concerning past device searches, and “may” rely on them when deciding to conduct another device search, “[p]laintiffs face a higher risk” for a future search than the general public. Pls.’ MSJ at 30. But this is incorrect. In reality, during the traveler’s initial encounter at the border, with rare exceptions, CBP Officers have access to only a limited set of information concerning a

*v. Mallinckrodt, Inc.*, 471 F.3d 277, 284 (1st Cir. 2006) (holding that probabilistic injury requires “a substantial probability that harm will occur”).

The First Circuit has held that while “probabilistic injury” could theoretically support standing in certain contexts, “not all risks constitute injury.” *Kerin v. Titeflex Corp.*, 770 F.3d 978, 983 (1st Cir. 2014). And the First explicitly rejected standing founded on “remote” risks or an “exceedingly low probability” of harm. *Id.* Under any reasonable definition, a less than 1-in-10,000 chance of a future search is an exceedingly low probability. Thus, judgment should be entered for the Government on the claims presented by these seven Plaintiffs.

Nor can Plaintiffs show standing as to the four individual Plaintiffs whose devices were searched more than once at the border. Of the four, Plaintiffs aver that three were searched twice, but point to no search more recent than August of 2017. Given the fact that none of these three Plaintiffs have experienced any searches in nearly two years, while they claim “to regularly travel outside the country,” Am. Compl. ¶ 2, they have not established that they are at substantial risk for such searches in the immediate future.<sup>14</sup> *See Conservation Law Found. v. Pub. Serv. Co. of N.H.*, No. 11-CV-353-JL, 2012 WL 4477669, at \*11 (D.N.H. Sept. 27, 2012) (denying standing to seek injunctive relief where most recent injury was over two years prior). And Plaintiff Merchant, the sole plaintiff who has experienced a search more recently, has travelled at

---

given traveler, which does not include whether he or she was previously the subject of a border device search. *See* Howe Decl. ¶¶ 12-13. In the vast majority of circumstances, then, a past device search will not increase the risks of a future search, and Plaintiffs fail to provide any evidence to the contrary.

<sup>14</sup> Many of these individual Plaintiffs have travelled internationally multiple times. For example, Plaintiff Bikkanavar has taken 35 international trips and his only search was in 2016. Ex. J, Bikkanavar Resp. to Interrogs. 1, 4; Bikkanavar Suppl. Resp. to Interrogs 1, 4. Plaintiff Wright has travelled internationally 21 times and his last search was also in 2016. Ex. J, Wright Resp. to Interrogs. 1, 4 Wright Suppl.Resp. to Interrogs 1, 4.

least five times since her most recent search and has not been searched during any of those trips. *See Ex. J, Merchant Resp. to Interrogs. 1, 4; Merchant Suppl. Resp. to Interrogs 1, 4, 7.* She thus provides no basis for this Court to find that she is likely to be searched in the future, and accordingly lacks standing on that ground.

B. Plaintiffs Lack Standing to Seek Expungement

Plaintiffs' only other claimed basis of standing, expungement, is also improper here. Plaintiffs allege that Defendants are improperly retaining two types of information: (1) TECS records which contain information observed during the search of seven Plaintiffs' phones and (2) information copied from Plaintiff Wright's electronic device.<sup>15</sup>

Plaintiffs fail to describe any concrete and particularized injury resulting from the Government's retention of information. At most, Plaintiffs argue that the Government can retain the information and could possibly "use and exploit it," at some unknown point in the future, in some unspecified manner. Pls.' MSJ at 26. But a vague possibility that the Government might take some adverse action in the future is insufficient to support standing. *See Laird v. Tatum*, 408 U.S. 1, 13, (1972) (rejecting argument that standing could be based on "speculative apprehensiveness that the Army may at some future date misuse the information [acquired through surveillance activities] in some way that would cause direct harm to respondents").

Plaintiffs also cannot establish redressability. As this Court previously recognized, the relief of expungement is inherently contingent on the merits of a legal question, whether the

---

<sup>15</sup> Plaintiffs' claim that Defendants have retained Wright's data is based on an assumption that the absence of a specific document showing destruction means the data was not destroyed. However, as set forth in the Declaration of Jenny Tsang, *see Ex. L, CBP's San Francisco Laboratory deleted all copies of Wright's information that had been made.* Thus, there can be no material dispute of fact over this issue, as the information is uniquely within Defendants' knowledge. Regardless, any factual dispute should not preclude the entry of judgment for Defendants, for the reasons set forth above.

“retention of Plaintiffs’ data is . . . itself a violation of the Fourth Amendment[.]” Order at 27. Even if a search violates the Fourth Amendment, it is a separate question whether the Government may keep or use the obtained information, even in criminal proceedings. *See, e.g., Pa. Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 362 (1998). It would make little sense for this Court to order relief in the form of expungement when there is no showing as to why such information may not be lawfully retained.<sup>16</sup> *Cf. Scott*, 524 U.S. at 363 (noting that illegally obtained evidence need not even be suppressed in grand jury proceedings, civil tax proceedings and civil deportation proceedings). Thus, because this Court cannot redress the purported injury of information retention through Plaintiffs’ claims, redressability is lacking here as well. *See Katz v. Pershing, LLC*, 672 F.3d 64, 72 (1st Cir. 2012) (“[P]laintiff must show that a favorable resolution of her claim would likely redress the professed injury.”).

### CONCLUSION

For the foregoing reasons, this Court should grant summary judgment to Defendants and deny Plaintiffs’ Motion for Summary Judgment.

Dated: June 6, 2019

Respectfully submitted:

JOHN R. GRIFFITHS  
Director, Federal Programs Branch

---

<sup>16</sup> Such relief would also potentially violate the Federal Records Act and accompanying Records Disposal Act, 44 U.S.C. § 3314, which “provides the exclusive means for record disposal.” *Kissinger v. Reporters Comm. for Freedom of the Press*, 445 U.S. 136, 147-48 (1980). There can be no reasonable dispute that TECS records constitute federal records, such that their destruction may only be carried out pursuant to the agency regulations and policies established pursuant to statute. Moreover, destruction of federal records would pose numerous problems, as it would effectively obliterate the evidence that Plaintiffs’ searches ever occurred, making these records inaccessible by future requesters under the Freedom of Information Act, as well as threatening accurate recordkeeping, which benefits internal audits.



DIANE KELLEHER  
Assistant Director, Federal Programs Branch

/s/ Marsha Edney  
MARSHA STELSON EDNEY  
Senior Trial Counsel

MICHAEL DREZNER  
Trial Attorney  
U.S. DEPARTMENT OF JUSTICE  
Civil Division/Federal Programs  
1100 L. St. NW  
Washington, DC 20005  
T: (202) 514-4505  
Email: Michael.Drezner@usdoj.gov

Attorneys for Defendants