Nos. 20-1077, 20-1081

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

GHASSAN ALASAAD; NADIA ALASAAD; SUHAIB ALLABABIDI; SIDD BIKKANNAVAR; JEREMIE DUPIN; AARON GACH; ISMAIL ABDEL-RASOUL, a/k/a Isma'il Kushkush; DIANE MAYE ZORRI; ZAINAB MERCHANT; MOHAMMED AKRAM SHIBLY; MATTHEW WRIGHT,

Plaintiffs-Appellees/Cross-Appellants,

v.

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

Defendants-Appellants/Cross-Appellees.

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

CORRECTED APPELLANTS' PRINCIPAL BRIEF

JOSEPH H. HUNT
Assistant Attorney General

ANDREW E. LELLING
United States Attorney

SCOTT R. McINTOSH
JOSHUA WALDMAN
Attorneys, Appellate Staff
Civil Division, Room 7232
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 514-0236

TABLE OF CONTENTS

Page

STATEMENT OF JURISDICTION 1

STATEMENT OF THE ISSUE 1

STATEMENT OF THE CASE 1

A. Legal Background 1

1. Border Searches Generally 1

2. Border Searches of Electronic Devices 3

B. Factual Background 7

C. Prior Proceedings 9

SUMMARY OF ARGUMENT 13

STANDARD OF REVIEW 15

ARGUMENT 15

I. CBP AND ICE DIRECTIVES DO NOT VIOLATE THE FOURTH AMENDMENT 15

A. Border Searches Do Not Require Probable Cause or a Warrant 16

B. The CBP and ICE Directives Comply With Any Applicable Reasonable Suspicion Requirement 19

1. Courts Before and After *Riley* Permit Suspicionless Manual Searches of Electronic Devices at the Border and Some Require Individualized Suspicion for Forensic Searches 21

2. The CBP and ICE Directives' Level of Suspicion Comply with the Fourth Amendment 28

TABLE OF CONTENTS (CONT'D)

Page

3. The District Court Erred in Holding That Basic Searches Are Non-Routine Border Searches 35

II. BORDER SEARCHES OF ELECTRONIC DEVICES ARE NOT LIMITED TO DIGITAL CONTRABAND 40

III. THE DISTRICT COURT DID NOT ERR IN ESCHEWING RIGID RULES FOR THE LENGTH OF DETENTION OF ELECTRONIC DEVICES 47

CONCLUSION 50

CERTIFICATE OF COMPLIANCE

CERTIFICATE OF SERVICE

ADDENDUM

TABLE OF AUTHORITIES

Page(s)

Cases

Alliance To Protect Nantucket Sound, Inc. v. U.S. Dept. of Army,
398 F.3d 105 (1st Cir. 2005) 15

Almeida-Sanchez v. United States,
413 U.S. 266 (1973) 2, 7

Boyd v. United States,
116 U.S. 616 (1886) 42

Carpenter v. United States,
138 S. Ct. 2206 (2018) 9

Commercial Union Ins. Co. v. Pesante,
459 F.3d 34 (1st Cir. 2006) 13

MRCo, Inc. v. Juarbe-Jimenez,
521 F.3d 88 (1st Cir. 2008) 12

Riley v. California,
573 U.S. 373 (2014) 9, 19, 20, 28, 31, 33, 36

Scarfo v. Cabletron Systems, Inc.,
54 F.3d 931 (1st Cir. 1995) 13

United States v. Aigbekaen,
943 F.3d 713 (4th Cir. 2019) 30

United States v. Alfaro-Moncada,
607 F.3d 720 (11th Cir. 2010) 18

United States v. Arnold,
533 F.3d 1003 (9th Cir. 2008) 23, 38, 39

United States v. Barrow,
448 F.3d 37 (1st Cir. 2006) 39

TABLE OF AUTHORITIES (CONT'D)

Page(s)

Cases

United States v. Braks,
842 F.2d 509 (1st Cir. 1988) 17, 18

United States v. Brunette,
256 F.3d 14 (1st Cir. 2001) 39

United States v. Cano,
934 F.3d 1002 (9th Cir. 2019) 19, 25, 32, 39, 41, 43, 44, 45

United States v. Carter,
590 F.2d 138 (5th Cir. 1979) 18

United States v. Charleus,
871 F.2d 265 (2d Cir. 1989) 18

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013) (en banc) 23, 24, 30, 31, 32, 33, 34, 37, 38, 39

United States v. Flores-Montano,
541 U.S. 149 (2004) 2, 15, 16, 17, 22, 43

United States v. Fortna,
796 F.2d 724 (5th Cir. 1986) 47

United States v. Gurr,
471 F.3d 144 (D.C. Cir. 2006) 46

United States v. Ickes,
393 F.3d 501 (4th Cir. 2005) 25, 32, 38, 39

United States v. Kolsuz,
890 F.3d 133 (4th Cir. 2018) 19, 26, 27, 29, 30, 31, 37, 38, 46

United States v. Linarez–Delgado,
259 Fed. Appx. 506 (3d Cir. 2007) 25

TABLE OF AUTHORITIES (CONT'D)

Page(s)

Cases

United States v. Molina-Gomez,
781 F.3d 13 (1st Cir. 2015) 28, 47

United States v. Molina-Isidoro,
884 F.3d 287 (5th Cir. 2018) 19, 27, 42

United States v. Montoya de Hernandez,
473 U.S. 531 (1985) 2, 16, 17, 22, 37, 43, 45, 48, 49

United States v. Oyekan,
786 F.2d 832 (8th Cir. 1986) 18

United States v. Ramos-Sanez,
36 F.3d 59 (9th Cir.1994) 17

United States v. Ramsey,
431 U.S. 606 (1977) 17, 40

United States v. Seljan,
547 F.3d 993 (9th Cir. 2008) 18

United States v. Stewart,
729 F.3d 517 (6th Cir. 2013) 27, 28

United States v. Touset,
890 F.3d 1227 (11th Cir. 2018) 21, 22

United States v. Uribe–Galindo,
990 F.2d 522 (10th Cir.1993) 17

United States v. Vergara,
884 F.3d 1309 (11th Cir. 2018) 19

United States v. Wanjiku,
919 F.3d 472 (7th Cir. 2019) 19, 21, 27, 32, 39

TABLE OF AUTHORITIES (CONT'D)

Page(s)

Cases

United States v. Wardlaw,
576 F.2d 932 (1st Cir. 1978) 17

United States v. Whitted,
541 F.3d 480 (3d Cir. 2008) 18

Vaqueria Tres Monjitas, Inc. v. Pagan,
748 F.3d 21 (1st Cir. 2014) 35

Warden v. Hayden,
387 U.S. 294 (1967) 42

Whren v. United States,
517 U.S. 806 (1996) 46

Statutes

6 U.S.C. § 211 2

8 U.S.C. § 1225 2

8 U.S.C. § 1357 2

19 U.S.C. § 482 2

19 U.S.C. § 507 2

19 U.S.C. § 1461 2

19 U.S.C. § 1496 2

19 U.S.C. § 1581 3

19 U.S.C. § 1582 3

19 U.S.C. § 1589a 3

TABLE OF AUTHORITIES (CONT'D)

Page(s)

Statutes

19 U.S.C. § 1595a 3

28 U.S.C. § 1291 ..... 1, 12

28 U.S.C. § 1292(a) 1

28 U.S.C. § 1292(a)(1) 12

28 U.S.C. § 1331 1

Regulations

19 C.F.R. § 161.2 3

19 C.F.R. § 162.6 3

22 C.F.R. § 127.4 3

REASONS WHY ORAL ARGUMENT SHOULD BE HEARD

This Court should hear oral argument in these cross-appeals, which present important Fourth Amendment questions of first impression in this Circuit.

STATEMENT OF JURISDICTION

Plaintiffs invoked the district court's jurisdiction under 28 U.S.C. § 1331. Appendix ("App.") 25 ¶ 11. The district court granted summary judgment to plaintiffs on November 12, 2019, Addendum 2-48, and entered a Judgment awarding declaratory and permanent injunctive relief on November 21, 2019, Addendum 50-51. The Government filed a timely notice of appeal on January 10, 2020, App. 65-67, and plaintiffs filed a timely notice of cross-appeal on January 13, 2020, App. 68-69. This Court has jurisdiction under 28 U.S.C. §§ 1291 and 1292(a). *See infra* note 10.

STATEMENT OF THE ISSUE

U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement have adopted Directives setting forth procedures for conducting searches and seizures of electronic devices during border inspections. Some types of searches require reasonable suspicion of activity in violation of the laws enforced or administered by the agencies, while other types do not require suspicion. The question presented is whether those Directives violate the Fourth Amendment as applied to plaintiffs.

STATEMENT OF THE CASE

A. Legal Background

1. Border Searches Generally

"Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border." *United*

States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985). Such "[r]outine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *Id.* at 538. "[S]earches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004). The Government's "longstanding concern for the protection of the integrity of the border" extends, among other things, to the "the power of the Federal Government to exclude aliens from the country," *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973), as well as the "prevent[ion of] the introduction of contraband into this country," the requirement for a person "entering the country to identify himself as entitled to come in," and "the collection of duties." *Montoya de Hernandez*, 473 U.S. at 537-38 & n.1. Accordingly, "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," in part because "the expectation of privacy [is] less at the border than in the interior." *Id.* at 539-40.

U.S. Customs and Border Protection ("CBP") and U.S. Immigration and Customs Enforcement ("ICE"), components of the Department of Homeland Security, are authorized to inspect and examine all individuals and merchandise entering or departing from the United States, including all types of personal property. *See, e.g.,* 6 U.S.C. § 211; 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. §§ 161.2, 162.6. 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, and laws relating to national security and terrorism, as well as regulatory and enforcement efforts in areas such intellectual property rights, food and drug safety, agriculture, and vehicle emissions standards. App. 221 ¶ 7; 238-239 ¶¶ 5, 9.

2. Border Searches of Electronic Devices

a. *CBP's Directive*

CBP's Directive, adopted on January 4, 2018, "governs border searches of electronic devices" to which all CBP Officers or "or any other official of CBP authorized to conduct border searches" "shall adhere." Addendum 52-53 §§ 2.2, 2.3, 3.1.[1] A "border search" includes "any inbound or outbound search pursuant to longstanding border search authority and conducted at the physical border, the functional equivalent of the border, or the extended border, consistent with law and agency policy." Addendum 53 § 2.3. An "electronic device" includes "[a]ny device that may contain information in an electronic or digital form, such as computers,

[1] CBP's 2018 Directive supersedes earlier-issued directives including its prior 2009 Directive, Addendum 63 § 11, which had permitted officers to conduct all border searches of electronic devices without suspicion, D. Ct. Dkt. 98-5 at 3 § 5.1.2; *see generally* App. 76-79 (comparing CBP's 2018 and 2009 directives).

tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players." Addendum 53 § 3.2.

CBP's Directive distinguishes between "basic" and "advanced" searches of electronic devices. An "advanced search" is "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." Addendum 56 § 5.1.4. A "basic search" is "[a]ny border search of an electronic device that is not an advanced search." Addendum 55 § 5.1.3. CBP officers may conduct a basic search "with or without suspicion," but may conduct an advanced search only if "there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern," and only with supervisory approval. Addendum 55-56 §§ 5.1.3, 5.1.4. *See* Addendum 5. For both searches, CBP officers may examine "only the information that is resident upon the device" and may not intentionally access "information that is solely stored remotely." Addendum 55 § 5.1.2.

CBP officers may "detain electronic devices * * * for a brief, reasonable period of time to perform a thorough border search," which "ordinarily should not exceed five (5) days." Addendum 58 § 5.4.1. To detain devices after an individual departs from a port of entry or other location of detention, a CBP officer must obtain supervisory approval, and any detention exceeding fifteen days requires a higher level of supervisory approval and re-approval every seven days. Addendum 58 § 5.4.1.1.

If, after review of the electronic device, an officer determines that there is "probable cause to believe that the device * * * contains evidence of a violation of law that CBP is authorized to enforce or administer," CBP may "seize and retain an electronic device." Addendum 60 § 5.5.1.1.

b. *ICE's Directive*

ICE's Directive, effective on August 18, 2009, "establishes policy and procedures * * * with regard to border search authority to search, detain, seize, retain, and share information contained in electronic devices possessed by individuals at the border, the functional equivalent of the border, and the extended border" and "applies to searches of electronic devices of all persons arriving in, departing from, or transiting through the United States, unless specified otherwise." Addendum 64 § 1.1. It defines "electronic device" to mean "[a]ny item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices." Addendum 65 § 5.2.

By supplemental guidance issued on May 11, 2018, ICE adopted the CBP Directive's distinction between "basic" and "advanced" searches, and requires reasonable suspicion of activity in violation of the laws enforced or administered by

ICE before conducting an advanced search. Addendum 5, 21; Addendum 74-75; App. 161 ¶ 9; 240 ¶ 11; 249 ¶ 1; 251 ¶ 14.[2]

Electronic devices "may be detained for further review," but searches "are to be complete[d] * * * in a reasonable time given the facts and circumstances of the particular search," and "generally * * * within 30 calendar days of the date of detention, unless circumstances exist that warrant more time." Addendum 67-68 § 8.1.4, 8.3.1. Any detention longer than 30 days requires supervisory approval, and re-approval at least every 15 days thereafter. Addendum 68 § 8.3.1.

c. *Statistics on Border Searches of Electronic Devices*

On a typical day, CBP is responsible for inspecting and establishing the admissibility of over 1 million travelers and over $7.5 billion worth of imported products. App. 230 ¶ 33. In fiscal year 2017, CBP processed more than 397 million arriving international travelers. During that time period, CBP conducted 30,524 border searches of electronic devices, meaning that approximately 0.007% of arriving international travelers processed by CBP officers had their electronic devices searched. App. 251 ¶ 13. Fewer than 3,500 of those searches were advanced searches. App. 165 ¶ 30. In the same time period, ICE conducted 681 advanced

[2] ICE's supplemental guidance supersedes in part its 2009 Directive permitting all border searches of electronic devices to be conducted without suspicion. Addendum 64 § 3; App. 74-76 (discussing ICE's 2009 Directive).

searches. ICE does not track the number of basic searches it conducts. App. 251 ¶¶ 14-15.

B. Factual Background

Plaintiffs are ten U.S. citizens and one lawful permanent resident. Each plaintiff alleges that his or her electronic devices were searched at the border on at least one occasion, and for some plaintiffs more than once.[3] All plaintiffs allege that their searches were conducted entirely by CBP officers, except for plaintiff (Matthew Wright) who alleges a search of his electronic device by an ICE agent in 2016. App. 150 ¶ 147. All of plaintiffs' searches pre-date the 2018 revisions to CBP's Directive and ICE's supplemental guidance, except for two plaintiffs (Suhaib Allababidi and Zainab Merchant) who assert that their devices were searched in 2018 and 2019. App. 149 ¶¶ 140-142; 352 ¶ 125.1; *see* Addendum 31.

Plaintiffs provide only brief descriptions of the manner in which officers searched their electronic devices. Many assert that CBP officers "searched" their phones, without elaboration.[4] Some plaintiffs state that CBP officers conducted a "manual" search or "manually" searched their devices,[5] while others assert officers

---

[3] All of plaintiffs' searches occurred either at the border or upon arrival at an international airport, its functional equivalent. *Almeida-Sanchez*, 413 U.S. at 272-73.

[4] App. 145 ¶ 121; 145 ¶ 123; 147 ¶¶ 130, 132; 148 ¶¶ 134, 137; 149 ¶¶ 140, 141; 149-150 ¶¶ 144, 149; 352 ¶ 125.1.

[5] App. 145 ¶ 121; 146 ¶ 125; 148 ¶ 135; 152 ¶ 157.

conducted a "basic" search of their devices.[6] One plaintiff asserts that CBP officers "had used 'algorithms' to search the phone," while another contends that "an ICE agent attempted to image [his] laptop with MacQuisition software, and a CBP forensic scientist extracted data from the SIM card in [his] phone and from his camera."[7]

Three plaintiffs assert that their devices were "confiscated" and kept after they left the port of entry and were not returned for various periods of time – 12 days, 2 months, 56 days, and 10 months.[8]

Plaintiffs filed this action in 2017, arguing that searching their electronic devices at ports of entry into the United States violates the Fourth Amendment unless those searches are conducted pursuant to a warrant and a showing of probable cause. App. 60 ¶¶ 168-169. Plaintiffs also alleged that prolonged seizure of their electronic devices violates the Fourth Amendment, and that the searches violate their First Amendment rights to the extent those devices "contain expressive content and associational information." App. 61 ¶¶ 171, 173. Plaintiffs sought declaratory and injunctive relief, as well as expungement of the records of any searches unlawfully conducted. App. 61-63.

---

[6] App. 147 ¶ 129; 149 ¶ 142.

[7] App. 146 ¶ 127; 150 ¶147.

[8] App. 152 ¶¶ 152, 154; 153 ¶¶ 160, 161, 166.

C. Prior Proceedings

On May 9, 2018, the district court denied the Government's motion to dismiss. The court held that plaintiffs have standing, App. 86-96, and "have plausibly alleged a Fourth Amendment claim here," App. 114.

On November 12, 2019, the district court granted summary judgment to the plaintiffs in part. Addendum 2-49. The court reiterated its earlier conclusion that plaintiffs have standing to seek prospective relief and expungement of any unlawfully obtained records. Addendum 8-15.

The district court held that the CBP and ICE Directives violate the Fourth Amendment as applied to plaintiffs. The court recognized that border searches are an exception to the Fourth Amendment's usual warrant requirement, and that no suspicion is required for "routine" border searches. Addendum 16, 22. The court concluded, however, that searches of electronic devices – whether "basic" or "advanced" – are non-routine border searches. Addendum 30-34. Relying on *Riley v. California*, 573 U.S. 373 (2014), and *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the court emphasized the substantial personal privacy interests implicated by the searches of electronic devices capable of storing so much personal information. Addendum 30 The court underscored that "[s]uch information can be accessed during not just the forensic searches [*i.e.*, advanced searches] under the CBP and ICE policies, but also under a basic search." Addendum 30; Addendum 34 ("The concerns laid out in Riley * * * apply with equal force to basic and advanced searches.").

While the court rejected plaintiffs' argument that the Fourth Amendment requires a warrant and probable cause to conduct these non-routine searches, it held that both basic and advanced searches require reasonable suspicion. Addendum 34-39. The court exempted "cursory search[es]," which entail "a brief look reserved to determining whether a device is owned by the person carrying it across the border, confirming that it is operational and that it contains data," holding that such searches do "not require a heightened showing of cause." Addendum 31.[9]

The district court placed an additional limitation on border searches of electronic devices. It reasoned that the purpose of the border search exception to the Fourth Amendment is to interdict contraband itself, not to discover evidence about the importation of contraband or other border-related crimes. Addendum 18, 36. Accordingly, the court held that officers must have reasonable suspicion that the electronic devices contain digital contraband itself – for example, child pornography, classified information, or counterfeit media, Addendum 21-22 – rather than reasonable suspicion that the devices contain evidence about past or future crimes, including crimes relating to contraband crossing the border, Addendum 36.

---

[9] Although the district court's declaratory judgment expressly exempted cursory searches, its injunctive order did not. Addendum 51.

The district court also excepted CBP searches premised on a "national security concern" to the extent "it is akin to the well-recognized 'exigent circumstances' exception to the warrant requirement," Addendum 21 n.5, but that exception is not included in the district court's declaratory judgment or injunctive order.

As to plaintiffs' claims that the Government violates the Fourth Amendment by prolonged seizure of their devices, the court concluded that the length of a reasonable seizure is not amenable to a fixed rule. Instead, the court held only that where an electronic device is seized pursuant to reasonable suspicion, the detention "must be for a reasonable period that allows for an investigatory search for contraband." Addendum 43.

Concerning plaintiffs' First Amendment claim, the court noted that the agencies' Directives are content-neutral on their face, and "it is not clear what less restrictive means could be employed" in this context. Addendum 40-41. Particularly because the court already required reasonable suspicion for all non-cursory searches, the court held that any First Amendment burdens from such a search are already justified by the heightened showing required for a border search of electronic devices. Addendum 41.

The court also declined, as a matter of discretion, to order the equitable remedy of expungement. Addendum 44-47.

The court held that while declaratory relief was appropriate at that time, it would not enter any injunctive relief absent further briefing, Addendum 47-49, which the court subsequently ordered, D. Ct. Dkt. 110. The parties filed a Joint Statement in which both sides agreed that the district court should enter declaratory relief consistent with the court's opinion and injunctive relief limited to the named

plaintiffs. Neither party requested any further relief or action by the court. App. 356-359.

On November 21, 2019, the district court entered a judgment granting plaintiffs declaratory relief stating that the CBP and ICE Directives for basic and advanced searches violate the Fourth Amendment to the extent they do not require reasonable suspicion that the devices contain contraband. The court further granted injunctive relief enjoining the defendants from searching or seizing any electronic device belonging to a named plaintiff during an encounter at the border or its equivalent, unless the defendants have reasonable suspicion that the device contains contraband, and further enjoined defendants from detaining such a device for longer than a reasonable period that allows for an investigatory search for that contraband. Addendum 50-51.

The Government filed a timely notice of appeal on January 10, 2020, and plaintiffs filed a timely notice of cross-appeal on January 13, 2020. App. 65-69.[10]

[10] This Court has appellate jurisdiction over the district court's injunctive order pursuant to 28 U.S.C. § 1292(a)(1). Despite the fact that the district court granted plaintiffs' summary judgment motion only in part, and denied the Government's motion for summary judgment, Addendum 49, there is also a final judgment for purposes of 28 U.S.C. § 1291. While "[a] district court's order denying a motion for summary judgment is interlocutory and thus, in most cases, not appealable * * * [a]n order or judgment is usually considered 'final' (hence, appealable) * * * when it resolves the contested matter, leaving nothing to be done except execution of the judgment." *MRCo, Inc. v. Juarbe-Jimenez*, 521 F.3d 88, 93 (1st Cir. 2008). Thus, "following the denial of summary judgment," where the parties jointly stipulate "that there were no longer any factual matters to be resolved at a trial," the district court's

SUMMARY OF ARGUMENT

I. The CBP and ICE Directives do not violate the Fourth Amendment. The district court correctly rejected plaintiffs' argument for requiring a warrant and probable cause before officers may search an electronic device at the border. No court has ever imposed such a requirement in the context of a border search. Even for the most intrusive nonroutine border searches of a person, such as strip searches or involuntary x-rays, no more than reasonable suspicion is required.

The district court erred, however, in requiring reasonable suspicion for a basic search. Every circuit to address the question has rejected that approach, either holding that no suspicion is required for any search of property at the border, including electronic devices, or upholding suspicionless manual searches, in which officers simply look at pictures, videos, texts, or call logs on a device. This Court

---

judgment "based on undisputed facts" is final and appealable under 28 U.S.C. § 1291. *Commercial Union Ins. Co. v. Pesante*, 459 F.3d 34, 36-37 (1st Cir. 2006). *See Scarfo v. Cabletron Systems, Inc.*, 54 F.3d 931, 936-37 (1st Cir. 1995) (finding appellate jurisdiction where "a series of orders" issued by the district court were the "functional equivalent of a 'final judgment'" even though the orders were "not self-explanatory" and the court's disposition of each claim was "not explicitly stated" but finality was "[i]mplicit in those orders"). Here, neither the parties nor the district court contemplated a trial on any remaining disputed factual matters, and neither party in their Joint Statement requested any further action in this matter other than the entry of declaratory and injunctive relief consistent with the district court's opinion. In such circumstances, this Court may construe the district court's order as a final appealable judgment under Section 1291.

should resolve plaintiffs' claims by holding, in accord with all these circuits, that no suspicion is required for basic searches. As for advanced searches, this Court should hold, consistent with other cases, that even assuming advanced searches are nonroutine border searches and hence the Fourth Amendment would require reasonable suspicion, the CBP and ICE Directives comply with that more demanding level of suspicion. In this way, the Court can avoid unnecessarily resolving constitutional questions and the differences among those circuits.

II. The district court also erred in imposing an additional requirement that the border-search exception permits officers to search a device only for digital contraband, but not for evidence of a border-related offense. The district court premised its holding on Supreme Court precedent overruled more than fifty years ago. Its limitation does not make sense even on its own terms, because the purposes of the border-search exception apply equally to the search for contraband and the search for evidence of contraband smuggling or other border-related offenses. Finally, the district court's rule lacks clear guidance and invites inquiries into an officer's subjective intent, contrary to longstanding Fourth Amendment principles.

III. The district court correctly held that the Fourth Amendment does not establish any rigid rules on the length of time an electronic device may be detained during a border search. The Supreme Court has rejected hard-and-fast time limits, particularly at the border where the balance of interest leans heavily in the Government's favor and officers responsible for enforcing a broad array of border-

related restrictions must have reasonable flexibility to address the variety of potential threats they may encounter. Given the myriad potential threats posed by data on a device – from child pornography to information related to terrorism – officers require flexibility to ensure that the length of detention is adequate to the task. In addition, the length of a detention may vary depending on several factors, such as the limited resources for border agents responsible for processing more than 1 million travelers on a typical day, as well as difficulties caused by password protection, data encryption, and language translation. Finally, plaintiffs' privacy interests are minimal, as a detention implicates only their possessory interests in the devices themselves, not the detention of a person or the intrusiveness of the search of data.

STANDARD OF REVIEW

This Court reviews *de novo* the district court's grant of summary judgment, construing the evidence in the light most favorable to appellants. *Alliance To Protect Nantucket Sound, Inc. v. U.S. Dept. of Army*, 398 F.3d 105, 108 (1st Cir. 2005).

ARGUMENT

I. CBP AND ICE DIRECTIVES DO NOT VIOLATE THE FOURTH AMENDMENT

"The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *Flores-Montano*, 541 U.S. at 152. Accordingly, a person's "expectation of privacy [is] less at the border than in the interior," and "the Fourth Amendment balance between the interests of the

Government and the privacy right of the individual is * * * struck much more favorably to the Government at the border." *Montoya de Hernandez*, 473 U.S. at 539-540. The Supreme Court has reaffirmed "[t]ime and again" that routine "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *Flores-Montano*, 541 U.S. at 152-53. Thus, "[r]outine searches of the persons and effects of entrants [at the border] are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *Montoya de Hernandez*, 473 U.S. at 538. In addition, travelers "have a lesser expectation of privacy when they (or their goods) leave the country if for no other reason than the departure from the United States is almost invariably followed by an entry into another country which will likely conduct its own border search." *United States v. Boumelhem*, 339 F.3d 414, 423 (6th Cir. 2003).

In light of these longstanding precedents, the district court correctly rejected plaintiffs' argument that a border search of electronic devices requires a warrant and probable cause. However, the district court erred in holding that reasonable suspicion is required for both basic and advanced border searches of electronic devices.

A. Border Searches Do Not Require Probable Cause or a Warrant

Routine border searches do not require reasonable suspicion, probable cause, or warrant. *Montoya de Hernandez*, 473 U.S. at 538. The Supreme Court has noted the

possibility that "in the case of highly intrusive searches of the person," the "dignity and private interests of the person" might require "some level of suspicion," *Flores-Montano*, 541 U.S. at 152, but has reserved judgment on that question, *id.* at 154 n.2; *see Montoya de Hernandez*, 473 U.S. at 541 n.4; *United States v. Ramsey*, 431 U.S. 606, 618 n.13 (1977). On a single occasion the Supreme Court concluded that a person's *detention* during a border inspection was nonroutine, but was justified on a showing of "reasonable suspicion." *Montoya de Hernandez*, 473 U.S. at 543.

Following these precedents, this Court has held that a border search may be considered nonroutine based on a variety of factors, in particular "[t]he degree of invasiveness or intrusiveness associated with any particular type of search." *United States v. Braks*, 842 F.2d 509, 511 (1st Cir. 1988); *id.* at 512 (listing six factors). *Accord United States v. Uribe–Galindo*, 990 F.2d 522, 525–26 (10th Cir.1993); *United States v. Ramos-Sanez*, 36 F.3d 59, 61 (9th Cir.1994). But even for such nonroutine searches, this Court and others have required no more than reasonable suspicion.

For example, in *United States v. Wardlaw*, 576 F.2d 932, 934-35 (1st Cir. 1978), this Court held that a border search in which officers, suspecting that an individual was concealing contraband under her clothes, "command[ed]" her "to raise her skirts" and then "ordered [her] to disrobe completely," was justified on a showing of reasonable suspicion. This Court subsequently reaffirmed that "the only types of border search of an individual's person that have been consistently held to be non-

routine are strip-searches and body-cavity searches," and that "the 'reasonable suspicion' standard applies * * * to non-routine searches." *Braks*, 842 F.2d at 512-14.

Other circuits are in agreement that only highly intrusive inspections of the person, such as strip searches or body cavity searches, qualify as nonroutine border searches, and even then only reasonable suspicion is required. *United States v. Alfaro-Moncada*, 607 F.3d 720, 729 (11th Cir. 2010) ("Even at the border, however, reasonable suspicion is required for highly intrusive searches of a person's body such as a strip search or an x-ray examination."); *United States v. Seljan*, 547 F.3d 993, 1003 (9th Cir. 2008) ("a border search goes beyond the routine only when it reaches the degree of intrusiveness present in a strip search or body cavity search"); *United States v. Whitted*, 541 F.3d 480, 485-86 (3d Cir. 2008) ("body cavity searches, strip searches, and x-ray examinations are considered nonroutine by virtue of their significant intrusion on an individual's privacy" and therefore "require reasonable suspicion"); *United States v. Charleus*, 871 F.2d 265, 267 (2d Cir. 1989) ("More intrusive border searches of the person such as body cavities searches or strip searches, however, require at a minimum reasonable suspicion of criminal activity."); *United States v. Oyekan*, 786 F.2d 832, 837-38 (8th Cir. 1986) (strip searches and involuntary x-rays justified by reasonable suspicion); *United States v. Carter*, 590 F.2d 138, 139 (5th Cir. 1979) (strip search at border requires reasonable suspicion).

Thus, as the Seventh Circuit noted, "no court has ever required a warrant for any border search or seizure," and "no court has applied a standard higher than

reasonable suspicion for even highly intrusive searches at the border," and "no circuit court, before or after *Riley*, has required more than reasonable suspicion for a border search of cell phones or electronically-stored data." *United States v. Wanjiku*, 919 F.3d 472, 481, 483-84 (7th Cir. 2019). *See United States v. Cano*, 934 F.3d 1002, 1015 (9th Cir. 2019) ("post-*Riley*, no court has required more than reasonable suspicion to justify even an intrusive border search"); *United States v. Kolsuz*, 890 F.3d 133, 147 (4th Cir. 2018) ("Even as *Riley* has become familiar law, there are no cases requiring more than reasonable suspicion for forensic cell phone searches at the border."); *United States v. Molina-Isidoro*, 884 F.3d 287, 291-92 (5th Cir. 2018) ("For border searches both routine and not, no case has required a warrant. * * * [I]t is telling that no post-*Riley* decision issued either before or after this search has required a warrant for a border search of an electronic device."); *United States v. Vergara*, 884 F.3d 1309, 1312 (11th Cir. 2018) ("The forensic searches of Vergara's phones required neither a warrant nor probable cause"). Accordingly, the district court correctly rejected "the heightened warrant requirement supported by probable cause that Plaintiffs seek here." Addendum 39.

B. The CBP and ICE Directives Comply With Any Applicable Reasonable Suspicion Requirement

The district court nonetheless erred in holding that both basic and advanced searches of electronic devices are nonroutine border searches requiring reasonable suspicion. Addendum 22-39. The district court believed that *Riley v. California*, 573 U.S. 373 (2014), holding that the search of data on a cell phone seized during an arrest

requires a warrant and probable cause, is "particularly instructive." Addendum 26. *Riley* reasoned, in relevant part, that "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person," given their "immense storage capacity," their "pervasiveness," and their use to "collect[] in one place many distinct types of information * * * that reveal much more in combination than any isolated record" which increase the "consequences for privacy" resulting from a cell phone search. 573 U.S. at 393-95.

The district court's view that *Riley* requires reasonable suspicion for basic as well as advanced border searches of electronic devices is incorrect, and no appellate court has required reasonable suspicion for basic border searches, either before or after *Riley*. The Eleventh Circuit holds that no suspicion is required for a border search of electronic devices, while the Ninth Circuit holds that reasonable suspicion is required only for what it calls a "forensic" search, but not for "manual" searches. The Fourth Circuit agrees that officers may conduct suspicionless manual searches of electronic devices at the border, and holds that only a forensic search requires individualized suspicion, though it has declined to identify precisely what that heightened showing requires.

The CBP and ICE Directives require the level of suspicion called for by the most demanding Fourth Amendment standard adopted by these courts because they require reasonable suspicion for an advanced search of electronic devices. The district court erred in rejecting the holdings of these circuits and concluding that the CBP and

ICE Directives violate plaintiffs' Fourth Amendment rights by permitting suspicionless basic searches.

1. Courts Before and After *Riley* Permit Suspicionless Manual Searches of Electronic Devices at the Border and Some Require Individualized Suspicion for Forensic Searches

The Eleventh Circuit holds that "no suspicion is necessary to search electronic devices at the border." *United States v. Touset*, 890 F.3d 1227, 1229 (11th Cir. 2018). Although the Supreme Court has "required reasonable suspicion for the prolonged detention of a *person*" at the border, it "has never required reasonable suspicion for a search of property at the border, however non-routine and intrusive," and the court saw "no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property." *Id.* at 1233; *see id.* at 1234 ("Property and persons are different."); *Wanjiku*, 919 F.3d at 485 ("For non-destructive searches of property at the border, the [Supreme] Court required no particularized suspicion at all."). The Eleventh Circuit also explained that a "forensic search of an electronic device is not like a strip search or an x-ray" that would qualify as a nonroutine search, because "it does not require border agents to touch a traveler's body, to expose intimate body parts, or to use any physical force against him. Although it may intrude on the privacy of the owner, a forensic search of an electronic device is a search of property." *Touset*, 890 F.3d at 1234.

The Eleventh Circuit concluded that nothing in *Riley* requires a different rule. The Eleventh Circuit explained that *Riley* "involved the search-incident-to-arrest exception," the Supreme Court "expressly limited its holding" to that context, and therefore *Riley* "does not apply to searches at the border." *Id.* at 1234. Nor, in the border context, should "a traveler's privacy interest * * * be given greater weight than the paramount interest of the sovereign in protecting its territorial integrity," because "a traveler's expectation of privacy is less at the border." *Id.* at 1235; *see Flores-Montano*, 541 U.S. at 154 ("the expectation of privacy is less at the border than it is in the interior"); *Montoya de Hernandez*, 473 U.S. at 537 ("searches of persons or packages at the national border rest on different considerations and different rules of constitutional law from domestic regulations").[11]

Although the Ninth and Fourth Circuits have reached a different conclusion than the Eleventh Circuit, both courts have rejected the kind of across-the-board requirement of reasonable suspicion adopted by the district court in this case. Rather, both courts permit suspicionless "manual" searches, in which officers examine a device to view limited files, photos, or data. They require individualized suspicion only for "forensic searches" – searches where officers download and analyze a comprehensive catalog of data, including deleted information that may not be

[11] *Touset* held, in the alternative, that even if reasonable suspicion were required it was present under the circumstances. 890 F.3d at 1237-38.

accessed without the use of specialized equipment or software. Either view rejects the district court's requirement of reasonable suspicion even for basic searches.

For example, in *United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008), CBP officers searched the defendant's laptop computer at the border, not only to "see if it was functioning," but also to "open[] the files" on the computer in order to "view[] the photos" stored on it. *Id.* at 1005. The court held that no "particularized suspicion is required to search a laptop," *id.* at 1008, reasoning that because a person's expectation of privacy is significantly less at the border, a search of property, including the defendant's laptop, does not require individualized suspicion, especially where the laptop was neither damaged nor searched in a particularly offensive manner, *id.* at 1008-1010.

United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (en banc), involved two different searches of the defendant's electronic devices. In the first initial search, officers viewed photos on the defendant's electronic devices. *Id.* at 957-58. The court held that "the legitimacy of [that] initial search * * * is not in doubt," because the officers merely "turned on the devices and opened and viewed image files," and such a "quick look and unintrusive search of [a] laptop" is permissible "even without particularized suspicion." *Id.* at 960-61; *see also id.* at 960 n.6 (reaffirming *Arnold*'s holding that a "relatively simple search" at the border of a computer does not require reasonable suspicion); *id.* at 967 ("suspicionless searches of the type approved in *Arnold* will continue").

In the second search, ICE agents "used a forensic program to copy the hard drives of the electronic devices." *Id.* at 958. The court described a forensic search as "a powerful tool capable of unlocking password-protected files, restoring deleted material, and retrieving images viewed on web sites," *id.* at 957; *see id.* at 958 n.5, that is "comprehensive and intrusive [in] nature," and "cop[ies] the hard drive and then analyze[s] it in its entirety, including data that ostensibly has been deleted," *id.* at 962, in order to "mine every last piece of data on their devices," and make a "thorough and detailed search of the most intimate details" stored on those devices, *id.* at 967-68. The court held that such a "forensic examination" of a computer at the border requires reasonable suspicion. *Id.* at 962. The court reasoned that "[t]he private information individuals store on digital devices," including "the most intimate details of our lives," as well as their capacity for "storing warehouses full of information," *id.* at 964, implicate "significant expectation[s] of privacy," *id.* at 966, that requires reasonable suspicion, *id.* at 966-67. But the court emphasized the "commonsense differentiation between a manual review of files on an electronic device," which may proceed without any suspicion, and the "application of computer software to analyze a hard drive," which requires reasonable suspicion. *Id.* at 967.

The Ninth Circuit repeated these same distinctions in *United States v. Cano*, 934 F.3d 1002 (2019). The court noted that its decision in *Cotterman* "anticipated the Supreme Court's reasoning in *Riley*," *id.* at 1015, held that *Cotterman* applies to cell phones, *id.* at 1014-15 & n.7, and reiterated that "*manual* cell phone searches may be

conducted by border officials without reasonable suspicion but that *forensic* cell phone searches require reasonable suspicion" *id.* at 1007. *See id.* at 1008, 1019 ("[t]he validity of the manual search[]" in which an officer, "without any suspicion whatsoever," "briefly * * * reviewed" the cell phone's call log and text messages "is beyond dispute").

The Fourth Circuit takes a similar approach. In *United States v. Ickes*, 393 F.3d 501, 503 (4th Cir. 2005), the court considered a border search in which officers "confiscated a computer and approximately 75 disks" and then "search[ed] * * * the contents of his computer" to view various photographs and videos. The court held that such a search is permissible without suspicion, reasoning that under the border search exception, customs officers have broad authority and travelers have lower privacy expectations. *Id.* at 505-08. Although the court noted that the officers likely had reasonable suspicion, it held that was not required by the Fourth Amendment. *See id.* at 507 ("the probability that reasonable suspicions will give rise to more intrusive searches is a far cry from enthroning this notion as a matter of constitutional law").[12]

[12] In *United States v. Linarez–Delgado*, 259 Fed. Appx. 506, 507-08 (3d Cir. 2007) (unpublished), a customs officer searched a video on the defendant's camcorder. The court, relying on *Ickes*, rejected the defendant's Fourth Amendment challenge, observing that "[d]ata storage media and electronic equipment, such as films, computer devices, and videotapes, may be inspected and viewed during a reasonable border search." *Id.* at 508.

In *United States v. Kolsuz*, 890 F.3d 133 (4th Cir 2018), a CBP officer conducted a "'forensic' search," of the defendant's iPhone, which consisted of "attach[ing] the phone to a Cellebrite Physical Analyzer, which extracts data from electronic devices, and conduct[ing] an advanced logical file system extraction," a process that "lasted for a full month, and yielded an 896–page report that included [the defendant's] personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of [his] physical location down to precise GPS coordinates." *Id.* at 139.[13] The court held "that particularly in light of the Supreme Court's decision in *Riley*, a forensic border search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion." *Id.* at 144. The court explained that "[t]he sheer quantity of data stored on smartphones and other digital devices," combined with "the uniquely sensitive nature of th[e] information" stored on those devices and their "ubiquit[y]," means that when "[s]ubjected to comprehensive forensic analysis, a digital device can reveal an unparalleled breadth of private information." *Id.* at 145. The court thus held that "the forensic examination of [the defendant's] phone must be considered a

[13] CBP officers also conducted a "'manual' search" of the defendant's iPhone, which involved "scroll[ing] through [the defendant's] recent calls and text messages," *id.* at 139, but the defendant did not challenge the manual search on appeal, *id.* at 140 n.2, 141. The court of appeals nonetheless approvingly quoted the view of the district court in that case that the manual search was permissible under *Ickes*. *See Kolsuz*, 890 F.3d at 140, 142, 146 n.5.

nonroutine border search, requiring some measure of individualized suspicion." *Id.* at 137; *see id.* at 146 (same). While noting that "courts consistently have required only reasonable suspicion even when reviewing the most intrusive of nonroutine border searches and seizures," *id.* at 147, the court did not resolve whether a higher standard should apply because the case before it could be resolved on the basis of the good-faith exception to the exclusionary rule, *id.* at 147-48.

Judge Wilkinson, concurring in the judgment, agreed that "searches of cell phones and the like can reveal a trove of data * * * in a way that is deeply uncomfortable," but concluded "the ultimate question here is not whether there is a balance to be struck between what are highly significant privacy and security interests" but "what branch of government is best suited to make that determination," and he would have "defer[red] to the legislative and executive branches" in resolving that question in the first instance. *Kolsuz*, 890 F.3d at 152-53 (Wilkinson, J., concurring).[14]

---

[14] Other courts have addressed similar issues without squarely resolving the question. Both *United States v. Molina-Isidoro*, 884 F.3d 287, 290-93 (5th Cir. 2018), and *United States v. Wanjiku*, 919 F.3d 472, 479 (7th Cir. 2019), avoided the issue by relying on the good-faith exception to the exclusionary rule. *United States v. Williams*, 942 F.3d 1187, 1190-91 (10th Cir. 2019), concluded that officers had sufficient reasonable suspicion to satisfy any applicable constitutional requirement.

In *United States v. Stewart*, 729 F.3d 517 (6th Cir. 2013), the court upheld a border search by CBP and ICE officers in which they searched two of the defendant's computers by scrolling through pictures stored on the devices, but which was "not * * * a forensic examination." *Id.* at 521. While the court held that reasonable suspicion was not required, and "the government's border search of [the defendant's] computers did not violate his Fourth Amendment rights," *id.* at 526, the defendant

2. The CBP and ICE Directives' Level of Suspicion Comply with the Fourth Amendment

Although there are differences among the Fourth, Ninth and Eleventh Circuits regarding the Fourth Amendment standards applicable to border searches of electronic devices, the CBP and ICE Directives at issue in this case satisfy even the most demanding level of suspicion adopted by those courts for forensic searches, and all the courts agree that a manual search of an electronic device at the border requires no suspicion.

As discussed above, the agencies' Directives divide border searches into two categories: "basic" and "advanced" searches. An advanced search is one 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. An advanced search requires reasonable suspicion of activity in

---

conceded that the officer's search of his computer *at the airport* "was constitutionally permissible," *id.* at 525, and the court focused principally on rejecting the defendant's argument that conducting the same search at an ICE facility twenty miles away transformed it into an "extended border search" for which reasonable suspicion would be required, *id.* at 524-26.

In *United States v. Molina-Gomez,* 781 F.3d 13 (1st Cir. 2015), this Court found no Fourth Amendment violation for a border search of a laptop computer and Sony Playstation game console, *id.* at 15-16, but the search involved an inspection of hidden compartment in the equipment and "no data extraction was ever conducted," *id.* at 16-17, and consequently did not implicate any privacy concerns associated with data. *See Riley*, 134 S. Ct. at 2485 ("Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case.").

violation of the laws enforced or administered by those agencies. Any other search constitutes a basic search and may be conducted without suspicion. *See supra* at 4.

Although the labels used by the agencies' Directives (basic and advanced) differ from those used by the Fourth and Ninth Circuits (manual and forensic), the difference is largely a matter of nomenclature, not substance. For all practical purposes, any search of plaintiffs' devices that those courts have described as "forensic" would constitute an "advanced" search under the agencies' Directives, and therefore would be subject to a reasonable-suspicion requirement under the Directives. Conversely, any search of plaintiffs' devices that the agencies' Directives would call "basic" would also qualify as a "manual" search under those circuit's precedents. All three circuits permit suspicionless basic searches of electronic devices. As for advanced searches, the agencies' requirement of reasonable suspicion would meet the most demanding level of suspicion adopted by the Ninth Circuit.

The practical alignment of advanced searches and forensic searches was expressly recognized by the Fourth Circuit in *Kolsuz*. The Fourth Circuit there noted that CBP's 2018 revision to its Directive "adopted a policy that treats forensic searches of digital devices as nonroutine border searches, insofar as such searches now may be conducted only with reasonable suspicion of activity that violates the customs laws or in cases raising national security concerns." 890 F.3d at 146. Indeed, *Kolsuz* noted, although CBP's Directive "distinguish[es] instead between 'basic' and 'advanced' searches * * * the import is the same" because "'[b]asic' searches (like

those we term 'manual') are examinations of an electronic device that do not entail the use of external equipment or software and may be conducted without suspicion," and "'[a]dvanced' searches (like 'forensic' searches) involve the connection of external equipment to a device—such as the Cellebrite Physical Analyzer used on Kolsuz's phone—in order to review, copy, or analyze its contents, and are subject to the restrictions noted above." *Id.* at 146 n.6. *See United States v. Aigbekaen*, 943 F.3d 713, 718 n.2 (4th Cir. 2019) ("Unlike a 'manual' search of a digital device, a forensic search generally entails the connection of external equipment and/or the use of specialized software.").

The Fourth Circuit was correct that the regulatory definition of an advanced search generally encompasses forensic searches. The distinction between basic and advanced searches turns on whether an officer connects the device to external equipment to review, copy or analyze the contents of a device. As a practical matter, the kind of searches the Fourth and Ninth Circuits regard as "forensic," ones that involve comprehensive copying and analysis of all the data (including deleted data) on an electronic device, can be carried out only by connecting the device to external equipment, and thus also fall within the agencies' definition of an "advanced" search. *Cotterman* described a forensic search as "a powerful tool capable of unlocking password-protected files, restoring deleted material, and retrieving images viewed on web sites," *id.* at 957, with the ability to access "deleted files" that "cannot be seen or accessed by the user without the use of forensic software," *id.* at 958 n.5, resulting in a

search that is "comprehensive and intrusive [in] nature," which "cop[ies] the hard drive and then analyze[s] it in its entirety, including data that ostensibly has been deleted," *id.* at 962, in order to "mine every last piece of data on their devices," and make a "thorough and detailed search of the most intimate details" stored on those devices, *id.* at 967-68. Similarly, *Kolsuz* described a forensic search as one consisting of "attach[ing] the phone to a Cellebrite Physical Analyzer, which extracts data from electronic devices, and conduct[ing] an advanced logical file system extraction," a process that "lasted for a full month, and yielded an 896–page report that included [the defendant's] personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of [his] physical location down to precise GPS coordinates." 890 F.3d at 139. Given the "immense storage capacity" of modern cell phones, capable of storing "millions of pages of text, thousands of pictures, or hundreds of videos," *Riley*, 573 U.S. at 393-94, officers could hardly conduct such a comprehensive recording and analysis of a cell phone's data (to say nothing of a laptop computer's data) by hand, without the assistance of external equipment to copy and analyze that data, and both *Cotterman* and *Kolsuz* expressly observed that officers used external software or equipment to conduct forensic searches. Conversely, if an officer examines the device only by manual interaction unassisted by external equipment, he or she has little ability to generate the kind of comprehensive catalog of data that courts label as "forensic."

The limited nature of basic searches is reinforced by practical considerations of the agencies' resources and manpower. In theory, given unlimited time and resources, a single officer, or an army of them, could conduct "basic" searches, scrolling through all accessible data on a device by hand, recording it with pencil and paper, and later analyzing it in comprehensive fashion. But that is a fanciful scenario in practice. As noted above, *supra* at 6, CBP performed more than 30,000 border searches of electronic devices in 2017 alone, the vast majority of which were basic rather than advanced searches. Even with the assistance of external equipment or software, the kind of comprehensive analysis compiled by a forensic search can take "several hours," *Cotterman*, 709 F.3d at 958, or "weeks," *Cano*, 934 F.3d at 101, or even "months," *Wanjiku*, 919 F.3d at 477, to complete. To engage in that kind of comprehensive data collection and analysis by hand would place impossible demands on the agencies' resources. *Ickes*, 393 F.3d at 507 ("Customs agents have neither the time nor the resources to search the contents of every computer."); *Cotterman*, 709 F.3d at 978 (Callahan, J., concurring in part and dissenting in part) ("the government does not have the resources – time, personnel, facilities, or technology – to exhaustively search every (or even a majority) of the electronic devices that cross our borders"); App. 221 ¶ 8. Indeed, one reason why CBP's Directive requires officers who wish to conduct advanced searches to both satisfy the reasonable suspicion standard and also obtain supervisory approval, *see supra* at 4, is to ensure that this time-

consuming process is managed in a consistent and sensible way sensitive to the agencies' limited resources.

These kinds of practical restrictions have often informed the permissible scope of Fourth Amendment searches. As *Cotterman* noted, the privacy implications for any search of property has been "traditionally circumscribed" by practical considerations of "[t]he amount of private information [that can be] carried by international travelers" in an object "the size of the traveler's luggage or automobile." 709 F.3d at 964. And *Riley* likewise observed that "[b]efore cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy," because "[m]ost people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so." 134 S. Ct. at 2489. Sometimes, those practical realities might broaden a person's expectations of privacy; an electronic device's storage capacity, and its practical ability to contain a large amount of personal data, is one factor leading courts to recognize a greater privacy interest in their data. But the converse is true as well. Where CBP or ICE officers conduct a basic search without the assistance of external equipment, there is no practical possibility for them to engage in the comprehensive data collection entailed in a forensic search. This is another reason why any of plaintiffs' searches falling under the agencies' definition of a basic search would also qualify as a manual search as understood by the Fourth and Ninth Circuits, and why any of

plaintiffs' searches those courts would consider to be forensic would also qualify as an advanced search under the agencies' Directives.

Plaintiffs' own descriptions of their searches essentially acknowledge that, at least for the purposes of their claims, the agencies' Directives reflect the manual/forensic distinction adopted by the Fourth and Ninth Circuits. Plaintiffs largely describe their own searches using the labels "manual" and "basic" in seemingly interchangeable fashion. *See supra* at 7-8 & nn.5-6. To the extent that there may theoretically be unusual instances in which the agencies' distinction between basic and advanced searches would not perfectly align with the judicially developed manual/forensic distinction, plaintiffs' sparse descriptions of their own searches even after a full record was developed on summary judgment, *see supra* at 7-8, indicates that no such concerns are presented here.[15]

[15] To the extent the basic/advanced distinction does not identically match the manual/forensic distinction, the agencies' Directives may be *more protective* than the Fourth and Ninth Circuit would require as a constitutional matter. First, *Cotterman* would permit a forensic search that includes examination of data stored "[i]n the 'cloud,'" that is, "a user's data * * * held on remote servers rather than on the device itself." 709 F.3d at 965. But CBP searches, both basic and advanced, are limited to "only the information that is resident upon the device" and officers "may not intentionally use the device to access information that is solely stored remotely." Addendum 55 § 5.1.2. Second, it is possible that there may be advanced searches where the agencies connect external equipment yet conduct only a modest or less-than-comprehensive analysis; such searches would require reasonable suspicion under the agencies' Directives, even if the Fourth and Ninth Circuit would not require as much. *See, e.g.,* App. 146 ¶ 127; 328 ¶ 127 (claiming an advanced search lasting 19 minutes). Third, the Directives' distinction between basic and advanced searches provides a clearer brightline rule which may be more easily understood and applied by officers, enabling greater consistency and predictability in its application.

Because advanced searches under the agencies' Directives subsumes the types of searches courts would consider to be forensic, this Court can and should resolve the claims of the eleven plaintiffs before it by holding, consistent with all of these circuits, that the Fourth Amendment permits suspicionless basic searches of plaintiffs' electronic devices. As for advanced searches, this Court can and should dispose of this appeal by holding that, even assuming that reasonable suspicion is a constitutional requirement for advanced searches, the agencies' Directives satisfy any such Fourth Amendment mandate. In this way, the Court need not resolve the differences among the Fourth, Ninth, and Eleventh Circuit in the present case. Resolving the appeal in this fashion is consistent with the venerable principle of constitutional avoidance, *Vaqueria Tres Monjitas, Inc. v. Pagan*, 748 F.3d 21, 26 (1st Cir. 2014), is in accord with courts that have avoided resolution of this very issue on alternative grounds, *supra* note 14, and properly defers resolution of broader Fourth Amendment questions pertaining to border security policies to the elected executive and legislative branches, *Kolsuz*, 890 F.3d at 148-152 (Wilkinson, J., concurring in the judgment).

3. The District Court Erred in Holding That Basic Searches Are Non-Routine Border Searches

The district court concluded that "a basic search and an advanced search * * * implicate the same privacy concerns" and are thus both non-routine border searches. Addendum 30. It reasoned that a basic search could theoretically "reveal a wealth of personal information" and examine "a very large volume of information" using

keyword searches on the device itself. Addendum 30-31. The district court was "unable to discern a meaningful difference between the two classes of searches in terms of the privacy interests implicated," and concluded that because *Riley* applies "with equal force to basic and advanced searches," Addendum34, "even basic searches" at the border "are not * * * routine searches," Addendum 31.

As explained above, *supra* at 30-33, the district court's speculation that a trove of personal information might be compiled and analyzed by an officer (or team of officers) conducting a basic search by hand, unassisted by external equipment, is divorced from practical reality. There is no credible basis on which to believe that a basic search could practicably approach anything like a comprehensive forensic analysis that can access even deleted files. Indeed, assuming that in the border context the technological advancements of cell phones mean they should not be "lump[ed] together" with other "physical items," *Riley*, 573 U.S. at 393, it is difficult to see why the use of sophisticated external equipment and software in an advanced forensic search should be lumped together with a basic search in which officers might scroll through some data by hand. Nor would recognizing such a distinction "launch courts on a difficult line-drawing expedition," *id.* at 401, because there are no practical difficulties in determining whether officers connect a device to external equipment in order to review, copy and/or analyze its contents, and hence whether a search is basic or advanced.

Both the Fourth and Ninth Circuits hold that because a person's "expectation of privacy [is] less at the border than in the interior," and "the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is * * * struck much more favorably to the Government at the border," *Montoya de Hernandez*, 473 U.S. at 539-540, only the more intrusive forensic (or advanced) searches could possibly implicate sufficient privacy interests to alter the Fourth Amendment analysis. In *Cotterman*, the Ninth Circuit noted that when officers moved from a manual search of photos on the defendant's electronic devices, and into a comprehensive forensic examination, the search "transformed into something far different" and the court understood the "commonsense differentiation" between the two. *Cotterman*, 709 F.3d at 961, 968. And in *Kolsuz*, the Fourth Circuit distinguished the forensic search in that case from its prior decision in *Ickes* because the latter "did not address the use of the sophisticated forensic search methods at issue here." *Kolsuz*, 890 F.3d at 146 n.5. Judge Wilkinson's concurrence in *Kolsuz* expressly cautioned against reading the court's decision "to require individualized suspicion for border searches of all cell phones period," *id.* at 149, exactly the error committed by the district court below.

Even if there were some possible instance in which a basic search could approach the magnitude and scope of a forensic data analysis, that would not justify a reasonable-suspicion requirement for *every* basic search (or every basic search of plaintiffs' devices) regardless of how limited it may be, simply because of a theoretical

possibility that it could have been otherwise. And were such an aberrant factual pattern to arise in a different case, of course this Court could resolve it at that time.

Moving from the theoretical to the actual, the district court opined that "[t]he range of searches that Plaintiffs were subject to here illustrates this breadth" of basic searches. Addendum 31. But each example relied upon points to the opposite conclusion. The district court observed that in one search officers examined "photos, emails, and contacts," in another they searched "photographs" and "videos," and for a third plaintiff officers viewed "blog posts" and a "Facebook friends page," as well as (on a separate occasion) "emails and text messages." Addendum 32-33. But those facts do not meaningfully distinguish plaintiffs' cases from *Arnold*, where the court upheld the manual suspicionless border search of a laptop to "open[] the files" in order to "view[] the photos" stored on the device, 533 F.3d at 1005, and rejected the argument of greater privacy for "e-mail, internet chats and web-surfing habits," *id.* at 1006; or from *Cotterman*, where officers conducted a manual suspicionless border search in which they viewed photos on the defendant's devices, 709 F.3d at 957-58, and the court held that "the legitimacy" of that search "is not in doubt," because the officers merely "opened and viewed image files," and undertook a "quick look and unintrusive search of [a] laptop," *id.* at 960-61; or from *Ickes*, where the court upheld a manual suspicionless border search in which officers "search[ed] * * * the contents of [the defendant's] computer" to view various photographs and videos, 393 F.3d at 503. *See Kolsuz*, 890 F.3d at 139, 140 n.2 (defendant did not challenge a "'manual' search"

of the defendant's iPhone, in which officers "scroll[ed] through [the defendant's] recent calls and text messages").

The district court also noted that various searches took "thirty-seven minutes," "an hour," "one and a half hours," and "forty-five minutes." Addendum 32-33. But these facts actually demonstrate exactly the opposite point: their brief periods are a world apart from the forensic analyses described in other cases, which generally required "several hours," *Cotterman*, 709 F.3d at 958, if not "weeks," *Cano*, 934 F.3d at 101, or even "months," *Wanjiku*, 919 F.3d at 477, to complete.[16] Nor does it matter that one plaintiff's device contained "journalistic work-product" and "expressive content." Addendum 32. Even the district court agreed that the First Amendment does not require any additional protections for a search beyond what the Fourth Amendment would require. Addendum 42. *Accord United States v. Brunette*, 256 F.3d 14, 16 (1st Cir. 2001); *Arnold,* 533 F.3d at 1010; *Ickes,* 393 F.3d at 506-07. The district court thought it relevant that some devices were searched "out of [a plaintiff's] sight," Addendum 32, but that has no relevance to the Fourth Amendment analysis, *United States v. Barrow*, 448 F.3d 37, 41 (1st Cir. 2006) ("The testing of the contents of the

[16] The district court noted that two plaintiffs' phones were not returned for days or months. Addendum 32 n.6, 33. But a prolonged detention does not necessarily indicate a comprehensive search, as opposed to delays attributable to password protection or encryption, or the need to consult with translation services or subject matter experts. *See infra* at 49.

liquor bottles was clearly a routine border search, and we refuse to find it unreasonable merely because Barrow may not have been present."). The remaining factors noted by the district court – plaintiffs' occupations, the questions they were asked, and the fact that officers took notes – have no apparent relevance whatsoever to the breadth of the searches of plaintiffs' electronic devices.[17]

II. BORDER SEARCHES OF ELECTRONIC DEVICES ARE NOT LIMITED TO DIGITAL CONTRABAND

The district court also erred in holding that the border search exception permits officers to search electronic devices only for digital contraband, and does not permit them to "search [for] evidence of past or future crimes at the border." Addendum 36. Such a limitation would prohibit officers, based on the border-search exception, from searching an electronic device even with reasonable suspicion, unless officers were searching for digital contraband, such as child pornography, classified information, or counterfeit media. Addendum 21-22.[18] The district court mistakenly

---

[17] The district court noted that one plaintiff was told by CBP officers that they were using "'algorithms' to search his phone." Addendum 32. But that likely indicates it was an example of a forensic or advanced search, not a basic search. And that is exactly how plaintiff themselves viewed this search. App. 328 ¶ 127 (where "officers had used 'algorithms' to search the contents of the phone," plaintiffs understood this "to mean that they used one or more forensic tools").

[18] The district court's opinion does not address other recognized reasons for the border search exception, such as helping to determine the admissibility of travelers and national security concerns. *See, e.g., Ramsey*, 431 U.S. at 616, 620 (exception "grounded" in the "long-standing right of the sovereign" "to control * * * who and what may enter the country"). The Government does not construe the district court's

premised that limitation on precedent the Supreme Court overruled more than half a century ago. As other courts have correctly recognized, searches for contraband and searches for evidence of contraband and of other border-related offenses are equally within the border-search exception. And contrary to the district court's belief, its holding fails to provide clear guidance for law enforcement officers.

1. The district court reasoned that its holding "is consistent with the government's interest in stopping contraband at the border and the long-standing distinction that the Supreme Court has made between the search for contraband, a paramount interest at the border, and the search of evidence of past or future crimes at the border, which is a general law enforcement interest not unique to the border." Addendum 36. In so ruling, the district court relied on *United States v. Cano*, 934 F.3d 1002 (9th 2019), *petition for rehearing en banc pending*,[19] which held that "[t]here is a difference between a search for contraband and a search for evidence of border-related crimes," and "that the border search exception authorizes warrantless searches of a cell phone only to determine whether the phone contains contraband," *id.* at 1017. Both *Cano* and the district court, in turn, relied on *Boyd v. United States*, 116 U.S.

---

opinion as foreclosing reliance on those other grounds to sustain border searches of electronic devices in appropriate circumstances.

[19] The Government's petition for rehearing *en banc* in *Cano* is limited to the question of whether the border search of an electronic device is confined to a search for digital contraband, but does not seek rehearing of that court's distinction between manual and forensic border searches of electronic devices, discussed *supra* at 23-25.

616, 623 (1886), where the Supreme Court stated that "[t]he search for and seizure of stolen or forfeited goods, or 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." *See Molina-Isidoro*, 884 F.3d at 296 (Costa, J., concurring).

In *Warden v. Hayden*, 387 U.S. 294 (1967), however, the Supreme Court overruled precisely the distinction drawn in *Boyd*. The Court considered "the validity of the proposition that there is under the Fourth Amendment a distinction between merely evidentiary materials, on the one hand, * * * and on the other hand, those objects which may validly be seized including the instrumentalities and means by which a crime is committed, the fruits of crime." *Id.* at 295-96. The Court "reject[ed] the distinction* * * made by some of our cases between seizure of items of evidential value only and seizure of instrumentalities, fruits, or contraband" because it was "based on premises no longer accepted as rules governing the application of the Fourth Amendment." *Id.* at 300-01. Calling the distinction "wholly irrational" and "discredited," the Court explained that "[n]othing in the language of the Fourth Amendment supports the distinction between 'mere evidence' and instrumentalities, fruits of crime, or contraband," and "nothing in the nature of property seized as evidence renders it more private than property seized, for example, as an instrumentality; quite the opposite may be true." *Id.* at 301-02, 06.

2. As the district court recognized, Addendum 16-17, the border-search exception has been grounded in "the longstanding right of the sovereign" to "prevent[] the entry of unwanted persons and effects," *Flores-Montano*, 541 U.S. at 152, and "to prevent the introduction of contraband into this country," *Montoya de Hernandez,* 473 U.S. at 537. From that premise, the court then reasoned that "it is the interdiction of contraband, not the mere evidence of contraband, that is a paramount concern at the border, not evidence of contraband that might be helpful in the investigations of past or future crimes." Addendum 18; *see Cano*, 934 F.3d at 1016, 1018.

The district court's conclusion, however, does not follow from its premise. The sovereign's long-standing interest in controlling its own border and preventing harmful contraband from entering the country is implicated not only by a search for the contraband itself, but also by a search for evidence of schemes to smuggle contraband – which may lead to uncovering contraband or enable border agents to thwart such schemes – as well as other evidence of border-related offenses. The district court nowhere explained why the Government's interest in searching for contraband is "at its zenith at the international border," *Flores-Montano*, 541 U.S. at 152, yet that interest dissipates when officers search for evidence of contraband smuggling or other border-related offenses. As noted above, *supra* at 2-3, "CBP is responsible for enforcing criminal and civil laws and administering comprehensive regulatory schemes" in a variety of areas, including "those relating to immigration,

customs, international trade, child pornography, drug smuggling, weapons trafficking, financial crimes as well as national security and terrorism," and CBP likewise "enforces a host of other laws at the border on behalf of various federal agencies." App. 221 ¶ 7. The same is true for ICE, which "enforces a diverse portfolio of federal laws, including all types of cross-border criminal activity," such as "[h]uman smuggling and trafficking," "[t]ransnational gang activity," and "[i]nternational art and antiquity theft," as well as "regulatory and enforcement missions" extending to "food and drug safety, agriculture, and vehicle emissions standards." App. 238-239 ¶¶ 5, 9. A search for evidence of any such border-related offense falls well within the sovereign's interest in controlling its own border and the purposes of the border-search exception. Such searches for evidence of border-related offenses are not "untethered" to the purposes of the border-search exception. *Cano*, 934 F.3d at 1019.

The district court reasoned that without limiting border searches of electronic devices to digital contraband, the border search exception would authorize searches for general law enforcement purposes. Addendum 18, 36. *Cano* likewise reasoned that "border officials have no general authority to search for crime," and that without such a limitation, officers could search an electronic device even for evidence of a domestic crime such as price fixing. 934 F.3d at 1017. But that argument is a straw man. The CBP Directive at issue requires "reasonable suspicion *of activity in violation of the laws enforced or administered by CBP*, or in which there is a national security concern," Addendum 56 § 5.1.4 (emphasis added), and ICE's 2018 supplemental guidance is

similar, *see supra* at 5-6. Permitting searches for evidence of such border-related offenses in no way transforms the border-search exception into a license to search for evidence of any domestic crime or offense of any nature whatsoever.

3. The district court thought its ruling would "provide clear guidance to law enforcement," Addendum 37, but in fact it does the opposite. For example, in *Cano*, the court applied its distinction to uphold the suspicionless search of a cell phone's call log and text messages, but held that *taking notes* about those phone numbers has "no connection whatsoever to digital contraband" and thus was outside the border-search exception. 934 F.3d at 1019. That kind of fine distinction does not provide clear guidance for border officials who are responsible for inspecting over 1 million travelers on a typical day. Rather, it imposes the kind of "post hoc evaluations of police conduct" that the Supreme Court has cautioned against. *Montoya de Hernandez*, 473 U.S. at 542. Similarly, the district court distinguished between "the search for contraband" and "the search of evidence of *past or future crimes* at the border," Addendum 36 (emphasis added), just as the Ninth Circuit in *Cano* reasoned that "border searches * * * do not encompass searches for evidence of *past or future* border-related crimes," 934 F.3d at 1020 (emphasis added), suggesting that an officer may search the device for evidence that a person is engaged in smuggling contraband *at the moment of the border crossing* (for example, searching texts for evidence that the person is currently smuggling drugs). But such a distinction offers no clear guidance to officers, who cannot know beforehand whether any evidence of a border-related

offense stored on an electronic device will be of a past, present, or future violation, and attempting to ascertain the answer may lead to inquiries about an officer's subjective motivations that courts avoid under the Fourth Amendment. *Whren v. United States*, 517 U.S. 806, 813 (1996).

4. The district court's decision conflicts with *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018). *Kolsuz* agreed that "the scope of a warrant exception should be defined by its justifications" and that "[a]t some point * * * even a search initiated at the border could become so attenuated from the rationale for the border search exception that it no longer would fall under that exception." *Id.* at 143. But it held that "[t]he justification behind the border search exception is broad enough to accommodate not only the direct interception of contraband as it crosses the border, but also the prevention and disruption of ongoing efforts to export contraband illegally, through searches initiated at the border," and a cell phone search "conducted at least in part to uncover information about an ongoing transnational crime * * * fits within the core of the rationale underlying the border search exception." *Id.* at 143-44. *See also id.* at 147 n.7 (rejecting the argument "that even if the search of his phone could be justified by reasonable suspicion, what would be required is reasonable suspicion that contraband, as opposed to evidence, would be found on the device"). Other circuits also have held or indicated the border search exception permits searches for evidence besides contraband. *See, e.g., United States v. Gurr*, 471 F.3d 144, 149 (D.C. Cir. 2006) (affirming post-arrest border search of documents; "The

distinction [for border search purposes] * * * between contraband and documentary evidence of a crime is without legal basis."); *United States v. Fortna*, 796 F.2d 724, 738-39 (5th Cir. 1986) (copying documents that agents suspected "might relate to some illegal conduct involving material or persons entering or leaving the United States" was "clearly justified because [defendant] was crossing an international border"). *Cf. Molina-Gomez*, 781 F.3d at 17, 20 (concluding that text messages on cell phone properly contributed to reasonable suspicion that defendant was smuggling contraband).

III. THE DISTRICT COURT DID NOT ERR IN ESCHEWING RIGID RULES FOR THE LENGTH OF DETENTION OF ELECTRONIC DEVICES

In responding to plaintiffs' claims that prolonged detentions of their devices violate the Fourth Amendment, the district court noted that "the Supreme Court has been reluctant to adopt hard-and-fast time limits for the reasonableness of detention." Addendum 43. The district court was "reluctant to do so here," and held only that "such detention must be for a reasonable period that allows for an investigatory search for contraband." Addendum 43. As the court noted, CBP's Directive already specifies that it may "detain electronic devices * * * for a brief, reasonable period of time to perform a thorough border search," Addendum 58 § 5.4.1, and ICE's Directive specifies that searches "are to be complete[d] * * * in a reasonable time given the facts and circumstances of the particular search," Addendum 67 § 8.3.1.

Thus, the district court did not err to the extent it required the agencies to comply with their own existing policies.

The district court also reasoned that any further restriction on the duration of a device's detention was unnecessary "in light of its ruling as to the reasonable suspicion requirement for non-cursory border searches of electronic devices." Addendum 43. But the conclusion that the Fourth Amendment does not impose rigid rules for the length of time in which an electronic device is detained does not depend on the district court's mistaken belief that reasonable suspicion is required for basic searches.

In *Montoya de Hernandez*, the Supreme Court addressed the Fourth Amendment claim of a defendant who, at the border, was "detained incommunicado for almost 16 hours," in a manner that "was long, uncomfortable, indeed, humiliating." 473 U.S. at 542, 544. The Court noted it has "consistently rejected hard-and-fast time limits" on such detentions, because "common sense and ordinary human experience must govern over rigid criteria." *Id.* at 543. The Court held "that the detention in this case was not unreasonably long," in part because "[i]t occurred at the international border, where the Fourth Amendment balance of interests leans heavily to the Government," *id.* at 544, and because of the defendant's refusal to accept less time-consuming alternatives she was offered, *id.* at 543. The Court also held border officials "have more than merely an investigative law enforcement role" and are "also charged, along with immigration officials, with protecting this Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics,

or explosives." *Id.* at 544. The breadth of these responsibilities, and the potential harms these officers may encounter, demands rules that are flexible to the circumstances rather than rigid.

The same considerations apply here. Plaintiffs' devices were detained at the border, where the balance of interests leans heavily in the Government's favor. Given the possible threats presented by data on a device – anything from child pornography to unauthorized classified information to plans for building a bomb – the length of detention must be flexible to respond to the nature and scope of the potential threat posed, rather than imposing a rigid timeline. Moreover, the length of a detention may vary depending on several factors, such as border agent's limited resources, the fact that a device is password protected and/or encrypted, or the need for language translation services or subject matter experts. Addendum 57, 59 §§ 5.3.3, 5.4.2.1, 5.4.2.2. As in *Montoya de Hernandez*, travelers may be given an alternative, less-time consuming option – to give voluntarily the password to their device – and if they refuse, any extended seizure is at least partly attributable to that choice.[20] Finally, the detention at issue here is not of a *person*, but of property (an electronic device). And the length of that detention implicates only a plaintiffs' possessory interest in the

[20] Plaintiff Suhaib Allababidi, who alleges his devices were retained for two and ten months, App. 153 ¶¶ 160, 161, declined to unlock his phone for CBP officers, *see* D. Ct. Dkt. 91-2 at 2 ¶ 6. Plaintiff Matthew Wright, who allege his device was detained for 56 days, App. 153 ¶ 166, also declined to give CBP officers his password, *see* D. Ct. Dkt. 91-9 at 2 ¶ 6.

device; it does not implicate the privacy concerns noted in *Riley* relating to the data itself.

CONCLUSION

For the foregoing reasons, this Court should reverse and remand the judgment with instructions to enter summary judgment for the Government.

Respectfully submitted,

ANDREW E. LELLING
United States Attorney

SCOTT R. McINTOSH
JOSHUA WALDMAN
Attorneys, Appellate Staff
Civil Division, Room 7232
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 514-0236

May 2020

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limit of Federal Rule of Appellate Procedure 32(a)(7)(B) because it contains 12,904 words. This corrected brief also complies with the typeface and type-style requirements of Federal Rule of Appellate Procedure 32(a)(5)-(6) because it was prepared using Microsoft Word 2016 in Garamond 14-point font, a proportionally spaced typeface.

s/ Joshua Waldman
Counsel for Defendants-
Appellants/Cross-Appellees

CERTIFICATE OF SERVICE

I hereby certify that on June 1, 2020, I electronically filed the foregoing corrected brief with the Clerk of the Court for the United States Court of Appeals for the First Circuit by using the appellate CM/ECF system. Participants in the case are registered CM/ECF users, and service will be accomplished by the appellate CM/ECF system.

s/ Joshua Waldman
Counsel for Defendants-Appellants/Cross-Appellees

ADDENDUM

TABLE OF CONTENTS

1. District Court Opinion Awarding Summary Judgment,
District Court Docket 109 (Nov. 12, 2019)..... Addendum 2

2. District Court Judgment Awarding Declaratory and Injunctive Relief,
District Court Docket 112 (Nov. 21, 2019).....Addendum 50

3. U.S. Customs and Border Protection, CBP Directive No. 3340-049A,
Subject: Border Search of Electronic Devices (Jan. 4, 2018)
District Court Doekct 98-6.....Addendum 52

4. U.S. Immigration and Customs Enforcement, ICE Directive No. 7-6.1,
Directive Title: Border Searches of Electronic Devices (Aug. 18, 2009)
District Court Docket 98-4.....Addendum 64

5. Homeland Security Investigations, Message from the
AD of Domestic Operations,
Legal Update – Border Search of Electronic Devices (May 11, 2018)
District Court Docket 91-19.....Addendum 74

UNITED STATES DISTRICT COURT
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 ZORRI, ZAINAB MERCHANT, MOHAMMED AKRAM SHIBLY and MATTHEW WRIGHT,	
Plaintiffs,	
v.	**No. 17-cv-11730-DJC**
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.	

MEMORANDUM AND ORDER

CASPER, J. **November 12, 2019**

I. Introduction

Plaintiffs 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 (individually, by last name and collectively, "Plaintiffs") bring this suit against the following persons in their official capacities: Kirstjen

Nielsen, Secretary of the U.S. Department of Homeland Security ("DHS"),[1] Kevin McAleenan, Acting Commissioner of U.S. Customs and Border Protection ("CBP"), and Thomas Homan, Acting Director of U.S. Immigration and Customs Enforcement ("ICE") (collectively, "Defendants"). D. 7 at ¶¶ 14-26. Plaintiffs, ten U.S. citizens and one lawful permanent resident, allege that Defendants' conduct—searching Plaintiffs' electronic devices at ports of entry to the United States and, in some instances, confiscating the electronic devices being searched, pursuant to CBP and ICE policies—violates the Fourth Amendment (Counts I and III) and First Amendment (Count II) of the U.S. Constitution. D. 7 at ¶¶ 1-10, 168-73. They seek declaratory and injunctive relief related to Defendants' ongoing policies and practices as well as the searches of Plaintiffs' electronic devices including expungement of "all information gathered from, or copies made of, the contents of Plaintiffs' electronic devices, and all of Plaintiffs' social media information and device passwords." D. 7 at 40-42; D. 99 at 7-8, 12-13. Plaintiffs have now moved for summary judgment, D. 90, and Defendants have cross moved for summary judgment, D. 96. Although governmental interests are paramount at the border, where such non-cursory searches—even "basic" searches as broadly defined under CBP and ICE policies as well as the "advanced" searches of Plaintiffs' electronic devices—amount to non-routine searches, they require reasonable suspicion that the devices contain contraband. For the reasons stated below, the Court ALLOWS IN PART and DENIES IN PART Plaintiffs' motion, D. 90, and DENIES Defendants' motion, D. 96.

II. Standard of Review

The Court grants summary judgment where there is no genuine dispute as to any material

[1] The initial suit was filed against Elaine Duke, then Acting Secretary of DHS, but Defendants substituted Nielsen as Secretary of Homeland Security pursuant to Fed. R. Civ. P. 25(d). D. 15 at 9 n.1. Defendants have not made any further substitutions since then.

fact and the undisputed facts demonstrate that the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a). "A fact is material if it carries with it the potential to affect the outcome of the suit under the applicable law." Santiago-Ramos v. Centennial P.R. Wireless Corp., 217 F.3d 46, 52 (1st Cir. 2000) (quoting Sánchez v. Alvarado, 101 F.3d 223, 227 (1st Cir. 1996)). The movant "bears the burden of demonstrating the absence of a genuine issue of material fact." Carmona v. Toledo, 215 F.3d 124, 132 (1st Cir. 2000); see Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986). If the movant meets its burden, the non-moving party may not rest on the allegations or denials in her pleadings, Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 256 (1986), but "must, with respect to each issue on which she would bear the burden of proof at trial, demonstrate that a trier of fact could reasonably resolve that issue in her favor," Borges ex rel. S.M.B.W. v. Serrano-Isern, 605 F.3d 1, 5 (1st Cir. 2010). "As a general rule, that requires the production of evidence that is 'significant[ly] probative.'" Id. (alteration in original) (quoting Anderson, 477 U.S. at 249). The Court "view[s] the record in the light most favorable to the nonmovant, drawing reasonable inferences in his favor." Noonan v. Staples, Inc., 556 F.3d 20, 25 (1st Cir. 2009). On cross-motions for summary judgment, the standards of Rule 56 remain the same, and require the courts "to determine whether either of the parties deserves judgment as a matter of law on facts that are not disputed." Adria Int'l Grp., Inc. v. Ferré Dev., Inc., 241 F.3d 103, 107 (1st Cir. 2001).

III. Factual Summary

As perhaps evidenced by the parties' cross motions for summary judgment, the material facts concerning the searches of Plaintiffs' electronic devices and the policies pursuant to which CBP and ICE agents conduct border searches are undisputed. The Court gives this brief summary as background for the Plaintiffs' claims, but otherwise addresses the material facts in the analysis of the parties' respective legal positions below. This summary is drawn from the parties'

statements of material facts, D. 90-2, D. 98, and D. 103-1, as well as the parties' responses to those statements, D. 99-1 and D. 105.

The two agencies with primary responsibility for border searches are CBP and ICE. D. 90-2 at ¶¶ 1, 17; D. 98 at ¶ 1. Both agencies issued written policies on border searches of electronic devices in August 2009. D. 98 at ¶ 6; D. 99-1 at ¶ 6. In January 2018, CBP updated its policy to distinguish between two different types of searches, "basic" and "advanced," and to require reasonable suspicion or a national security concern for any advanced search, but no showing of cause for a basic search. D. 98 at ¶ 7; D. 99-1 at ¶ 7. Under this policy, an advanced search is defined 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." D. 98 at ¶ 8; D. 99-1 at ¶ 8. The parameters of an advanced search are clearer given this definition than that adopted for a basic search, which is merely defined as "any border search that is not an advanced search." D. 98 at ¶ 8; D. 99-1 at ¶ 8. Both CBP and ICE use the same definitions of basic and advanced searches and ICE policy also requires reasonable suspicion to perform an advanced search. D. 98 at ¶ 9; D. 99-1 at ¶ 9.[2]

The evidence as to the border searches of Plaintiffs' electronic devices is largely the same as alleged in the amended complaint and as relied upon by this Court in its Memorandum & Order regarding Defendants' motion to dismiss. Compare D. 34 at 10-16 with D. 99-1 at ¶¶ 120-149. Accordingly, the Court will not repeat all of the details of those searches again here but summarizes them and discusses some of them further below. Plaintiffs are U.S. citizens (except Dupin, who is a lawful permanent resident) who reside across the country and in Canada. D. 98 at ¶¶ 120, 124,

[2] The record appears silent on whether ICE policy also includes a national security concern exception for an advanced search. See D. 91-19; D. 99-1 at ¶ 18.

126, 128, 131, 133, 136, 143, 145, 148; D. 99-1 at ¶¶ 120, 124, 126, 128, 131, 133, 136, 143, 145, 148. Each of the eleven Plaintiffs has had their electronic devices searched at the border at least once. D. 98 at ¶¶ 51-52; D. 99-1 at ¶¶ 51-52. Some of the searches were at border crossings, id. at ¶¶ 121, 130, 135, 144, although most were at U.S. airports after a Plaintiff's return to the United States on an international flight. Id. at ¶¶ 123, 125, 127, 129, 132, 134, 137, 140, 141-42, 146, 149; D. 105 at ¶ 125.1; United States v. Molina-Gomez, 781 F.3d 13, 19 (1st Cir. 2015) (noting that "[i]nternational airports . . . are the 'functional equivalent' of an international border and thus subject to this [border search] exception"). These searches included searches of smartphones, either locked or unlocked, D. 99-1 at ¶¶ 121, 123, 125, 127, 129, 130, 132, 134, 135, 137, 140-42, 144, 147, 149, and at least as to Kushkush, Wright, and Allababidi, the search of other electronic media including, in some cases, laptop computers, id. at ¶¶ 134, 146-47; D. 105 at ¶ 125.1. Five of the Plaintiffs (Merchant, Nadia Alasaad, Dupin, Kushkush and Allababidi) have had their electronic devices searched more than once. D. 98 at ¶ 52; D. 99-1 at ¶ 52; D. 103-1 at ¶ 125.1; D. 105 at ¶ 125.1; D. 107 at 120-21. Two of the Plaintiffs, Merchant and Allababidi, have had their devices searched subsequent to the filing of the initial complaint in this case in September 2017: Merchant in September 2018, D. 98 at ¶¶ 53-54; D. 99-1 at ¶ 53, and Allababidi in July 2019, D. 103-1 at ¶ 125.1; D. 105 at ¶ 125.1. Each of the eleven Plaintiffs plans to continue to travel internationally with their electronic devices and many had or have international travel plans for later this year and into 2020. D. 99-1 at ¶¶ 170, 172, 174, 176, 178, 180, 182, 184, 186-87, 189.

Without recounting the nature and circumstances of all of the Plaintiffs' searches, a sample of them is illustrative. Nadia Alasaad has twice had her iPhones searched at the border over her religious objections to having CBP officers, especially male officers, view photos of her and her

daughters without their headscarves as required in public by their religious beliefs. D. 99-1 at ¶¶ 122-123. During the second search, which was of her daughter's phone, Alasaad alleges, and Defendants have not disputed, that a CBP officer mentioned a photograph that had been on Alasaad's phone during her earlier search but was not present in the second search. D. 91-1 at ¶ 24. Merchant is the founder and editor of a media website and has had her phones searched multiple times despite her concerns about officers seeing pictures of her without her headscarf on the phones and, on one occasion, her declining to give consent to search her phone since it contained attorney-client communications. D. 99-1 at ¶¶ 139, 142. Merchant observed a CBP officer viewing communications between her and her lawyer. D. 99-1 at ¶ 142. Dupin's phone contained information from his work as a journalist, D. 91-4 at ¶¶ 1, 4, while Bikkannavar's phone was a work phone officially owned by NASA's Jet Propulsion Laboratory, D. 99-1 at ¶ 7, and containing information from his work there, see id. at ¶¶ 7, 15.

It is also undisputed that information gleaned by CBP or ICE agents during certain of these border searches of Plaintiffs' electronic devices has been retained. Specifically, information observed by agents during the searches of the phones of Ghassan Alasaad, Nadia Alasaad, Bikkannavar, Dupin, Merchant, Shibly and Zorri has been retained. D. 99-1 at ¶ 150; D. 94. Reports containing such information note not just the fact that agents conducted a search of an electronic device, but in some instances, observations or characterizations of the information contained therein. See, e.g., D. 94 at 3 (noting absence of contraband from visual search of digital camera's contents), 94 (noting "no derogatory items [redacted] found"), 114 (noting "[n]o derogatory observed" during media examination), 127-28 (noting the contents of a social media post). A number of Plaintiffs had their electronic devices seized during the border searches, even if CBP later returned the devices to them. D. 99-1 at ¶¶ 152, 154, 156, 160-61, 162, 166. As to

one such Plaintiff, Wright, a computer programmer, CBP also extracted and retained data, including attempting to image his laptop with MacQuisition software and extracting data from the SIM cards in his phone and camera, D. 91-9 at ¶ 12, from his electronic devices, D. 99-1 at ¶ 151, and retained it for a period of fifty-six days, even if the parties agree that this data has now been returned to him. D. 98 at ¶ 166.

IV. Procedural History

Plaintiffs instituted this action on September 13, 2017. D. 1; D. 7. On May 9, 2018, after briefing and argument, the Court denied Defendants' motion to dismiss, D. 14, concluding that Plaintiffs had stated plausible Fourth Amendment and First Amendment claims and had standing to assert these claims and the requests for relief that they seek. D. 34. The parties each now move for summary judgment, D. 90; D. 96. The court heard the parties on the pending motions and took the matter under advisement. D. 106.

V. Discussion

A. Standing

As they did in their motion to dismiss, Defendants press their arguments challenging Plaintiffs' standing in their motion for summary judgment. Defendants primarily contend that the risk of future injury is too speculative to support standing with respect to border searches and certain deficiencies with respect to Plaintiffs' claim for expungement of data from previous border searches of their electronic devices retained by the government. On summary judgment, Plaintiffs "can no longer rest on . . . mere allegations" and must instead "set forth by affidavit or other evidence specific facts," to establish standing, "which for purposes of the summary judgment motion will be taken to be true." Lujan v. Defs. of Wildlife, 504 U.S. 555, 561 (1992) (internal citations and quotation marks omitted).

To establish Article III standing, Plaintiffs must demonstrate that they "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." Spokeo, Inc. v. Robins, __ U.S. __, 136 S. Ct. 1540, 1547 (2016), as revised (May 24, 2016).

1. Standing to Seek Injunctive or Declaratory Relief

In its ruling on Defendants' motion to dismiss, the Court ruled that Plaintiffs had demonstrated standing by plausibly alleging an injury in fact, traceable to the Defendants' alleged conduct that was likely to be redressed by a favorable decision by the Court. D. 34 at 17-24. Since Plaintiffs were seeking injunctive and declaratory relief, the Court also held that they had met their burden of showing that there was a substantial risk that the harm will occur in the future. Id. at 24. Concluding that the risk of a future search subject to ICE and CBP policies was higher for Plaintiffs than for the general population and rejecting Defendants' arguments that the allegations of such future harm were vague and speculative, id. at 20-24, the Court concluded that "Plaintiffs have plausibly alleged that they face a substantial risk of future harm from Defendants' ongoing enforcement of their border electronics search policies." Id. at 24.

On a more developed record, Defendants' challenge to Plaintiffs' standing now at the summary judgment stage fares no better. The nature of Plaintiffs' claimed injury remains the same (violation of constitutional rights as a result of electronic device searches conducted pursuant to official ICE and CBP border policies). Moreover, the record regarding the substantial risk of future harm has been borne out by discovery. The current record shows that agents have the potential to access information on a traveler's past searches and that such information may be used to inform decisions on future searches. D. 90-2 at ¶¶ 25-35; D. 98 at ¶¶ 25-35. At the border, both CBP and ICE have access to CBP's main database, TECS. D. 90-2 at ¶¶ 25-35; D. 98 at ¶¶ 25-35. TECS includes information about prior encounters between CBP and travelers at the border, including

but not limited to "lookouts" (alerts about a traveler or vehicle that have been entered in the database by either agency or other law enforcement agencies) and the reasons for, or information discovered in, prior broad searches of electronic devices. D. 90-2 at ¶¶ 27-28, 32; D. 98 at ¶¶ 27-28, 32. Agents and officers of both agencies may access and consider the information in TECS, including information about prior border searches, in deciding whether to conduct a border search of electronic devices. D. 90-2 at ¶¶ 34-35; D. 98 at ¶¶ 34-35. ICE also has its own database, Investigative Case Management ("ICM"). D. 90-2 at ¶ 45; D. 98 at ¶ 45. ICM contains information that ICE agents may access at the border including, but not limited to, prior encounters with travelers including whether they were subject to a device search. D. 90-2 at ¶ 49; D. 98 at ¶ 49. ICM can contain "an agent's description of data in a traveler's device, but not the data itself," but Defendants acknowledge that "ICM information about the contents of travelers' devices can be relevant to whether to conduct a future border search of an electronic device." D. 90-2 at ¶¶ 50-51; D. 98 at ¶¶ 50-51. Both CBP and ICE have access to CBP's Automated Targeting System ("ATS") that flags travelers for "additional inspection." D. 90-2 at ¶¶ 36, 44; D. 98 at ¶¶ 36, 44. Although ATS permits the officers to access dozens of other government databases, it also contains copies of data obtained from advanced searches of electronic devices obtained during prior border encounters. D. 90-2 at ¶¶ 40-41; D. 98 at ¶¶ 40-41. "ATS may use the information copied from a traveler's device to flag the traveler for heightened screening in the future." D. 90-2 at ¶ 43; D. 98 at ¶ 43.

This possibility, in light of the prior searches Plaintiffs have been subjected to and their future, anticipated international travel (as discussed below), translates into a sufficient likelihood that the challenged harm (i.e., search of electronic devices without cause) may occur for Plaintiffs in the future.

The recent additional search of Allababidi's devices on July 6, 2019 furthers Plaintiffs' argument as to the risk of future harm. Allababidi had previously been subject to a border search on January 24, 2017. D. 90-2 at ¶ 125. When he declined to provide the password to his locked phone, CBP seized it to conduct an examination. Id. at ¶ 125. On July 6, 2019, Allababidi arrived at the Toronto airport for a flight to Dallas, traveling with a smartphone and a laptop. D. 105 at ¶ 125.1. CBP officers searched both devices. Id. That such search of electronic devices continues for Plaintiffs, even in the midst of their ongoing legal challenges to same, serves as further, undisputed indication of the sufficient likelihood that, unremedied, such alleged harm will continue in the future, particularly given the Plaintiffs' future plans for international travel.

Defendants do not press the argument on summary judgment that Plaintiffs lack concrete plans for future international travel, but the Court notes that there is more than sufficient, undisputed evidence in the record as to both the frequency of Plaintiffs' international travel and the specific plans by many of the Plaintiffs to do so in the future, see D. 90-2 at ¶¶ 170, 172, 174, 176, 178, 182, 187, 189; D. 98 at ¶¶ 170, 172, 174, 176, 178, 182, 187, 189. For some examples, Bikkannavar has at least eight international trips planned by September 2020 to participate in solar car races and other related activities. D. 90-2 at ¶ 174; D. 98 at ¶ 174. Further, several of Plaintiffs have work or family commitments that require regular international travel, see, e.g., D. 99-1 at ¶¶ 176, 180, and Merchant lives in Canada but studies at university in Boston and will continue to do so until her graduation in May 2020, D. 99-1 at ¶ 182.

This likelihood of the future harm of Plaintiffs being subjected to searches of their electronic devices is not undermined, as argued by Defendants, by the fact that the overall percentage of such searches is low. Specifically, Defendants point to the stipulated facts here that of the hundreds of millions of international travelers processed by CBP in FY2017, for one

example, approximately .007% had their electronic devices searched. D. 98-7 at ¶ 13. Such evidence does not reduce the likelihood of future searches of these Plaintiffs for a number of reasons. First, the number of reported electronic devices likely is underestimated. Since the CBP calculated the total number of border searches of devices based upon closed or completed Electronic Media Reports ("EMRS"), D. 99-1 at ¶ 59, if the number of EMRs did not include all such searches, then this number may be underinclusive. The fact that there was no EMR as to the search of one of Plaintiff's smartphones (that of Nadia Alasaad on August 28, 2017, D. 99-1 at ¶ 61), suggests that this may be the case. Moreover, although CBP and ICE conduct such searches at the border, the number of searches cited above in FY2017 refers only to CBP searches and not ICE searches as ICE does not maintain records of the number of basic searches that it conducts. D. 98-7 at ¶ 14. ICE's recording of its advanced searches of electronic devices in FY2017—681—likely would be less than any number of basic searches of devices given that such basic searches do not involve the connection of external equipment to review, copy and analyze the device's contents in the way that advanced searches do. Accordingly, the total number of searches of electronic devices by both agencies is underinclusive and does not permit the Court to conclude that the total percentage of all electronic device searches is as low as .007%.

Second, even if this percentage were higher, but not a significant percentage of the total number of travelers admitted to the U.S. each year, the likelihood of Plaintiffs having their electronic devices searched without cause is not a remote risk or "exceedingly low probability" of harm. D. 97 at 38 (citing Kerin v. Titeflex Corp., 770 F.3d 978, 983 (1st Cir. 2014)). Although Defendants suggest the record only reveals that CBP and ICE officers may have access to the various agency databases, TECS, ATS and ICM, when conducting border searches, but not that they are accessed regularly in border encounters, D. 97 at 27 n.13, the record reasonably suggests

that a traveler who has previously had an electronic device searched in the past has some greater chance of having same done in the future. Even at primary inspection, CBP officers query TECS for "lookouts" and "recent border crossings," D. 99-1 at ¶ 29 and the TECS database includes information about prior border screenings. Id. at ¶ 34. The same is true as to secondary inspections as to the TECS database and its ATS database, which may contain copies of data from travelers' devices, id. at ¶ 41, ICE's ICM which contains information about prior border encounters "including whether travelers were subjected to device searches." Id. at ¶ 49. Given these practices and the fact that, as discussed above, several of the Plaintiffs have been searched multiple times, none of Defendants' arguments defeat standing.

For all of these reasons, the Court concludes that Plaintiffs have made sufficient showing of standing for the injunctive and declaratory relief that they seek.

2. Standing to Seek Expungement

Defendants also challenge Plaintiffs' standing to seek expungement. As Plaintiffs frame it now, they "seek to expunge information Defendants concede they retain." D. 99 at 12. Here, Plaintiffs seek to expunge information gathered from their electronic devices (and now memorialized in officers' reports, D. 94) and any copies made of their electronic devices, social media information and device passwords. D. 7 at 42. As previously noted in the Memorandum & Order regarding the motion to dismiss, D. 34 at 24, retention of data illegally obtained by law enforcement may constitute continuing harm sufficient to establish standing to seek expungement. See Tabbaa v. Chertoff, 509 F.3d 89, 96 n.2 (2d Cir. 2007) (stating that defendants there "properly do not contest that plaintiffs possess Article III standing based upon their demand for expungement" of data collected during border searches); Hedgepath v. Wash. Metro. Area Transit

Auth., 386 F.3d 1148, 1152 (D.C. Cir. 2004) (holding plaintiff had standing to seek expungement of arrest record).

Where, as here, Plaintiffs allege that such information and data was gathered as a result of the allegedly unconstitutional border searches and such harm could be addressed by expungement, contrary to Defendants' argument, D. 97 at 29-30, Plaintiffs have shown standing to seek expungement. While the ATS database appears to be the only database that may contain a copy of the data from an electronic device subject to an "advanced search," D. 90-2 at ¶¶ 40-41; D. 98 at ¶¶ 40-41, CBP and ICE retain the substance of data seized from both basic and advanced searches of electronic devices as an agent's description of same in the ICM database and TECS database could have been the result of either type of search. D. 90-2 at ¶¶ 26, 33, 50; D. 98 at ¶¶ 26, 33, 50. ICE policy permits retention of information from electronic devices that is "relevant to immigration, customs, and other law enforcement matters" and allows sharing of retained information with other law enforcement agencies. D. 99-1 at ¶¶ 22-23. CBP policy also permits retention of information on the same bases. D. 99-1 at ¶ 77. Specifically, the record indicates information retained from the device searches of the Alasaads, Bikkannavar, Dupin, Merchant, Shibly and Zorri. D. 99-1 at ¶ 150. Finally, Defendants retained information copied from Wright's devices but have since deleted all copies of Wright's data.[3] D. 99-1 at ¶ 55, 151. Accordingly, at least these Plaintiffs, therefore, had information gleaned from the search of their electronic devices that Defendants have retained. Here, such retention constitutes the alleged ongoing and future harm as such information can be accessed by border agents and may be relevant as to whether agents otherwise might conduct a future border search of an electronic device. D. 99-1 at ¶¶ 25-

[3]Wright has withdrawn his request for expungement. D. 98-12.

51. Accordingly, such Plaintiffs have standing to seek expungement, even as the Court reserves for discussion below whether this remedy is warranted here.

Having found standing as to Plaintiffs' claims, the Court now turns to the merits of their claims.

B. Plaintiffs' Fourth Amendment Claim (Count I)

The parties have cross-moved for summary judgment. Plaintiffs challenge both the constitutionality of their searches and they claim that CBP and ICE policies that allow for border searches of electronic devices without a warrant—even as these policies still require no showing (for "basic" searches) and now reasonable suspicion (for "advanced" searches, subject to a national security exception which would allow for an advanced search without reasonable suspicion)—are facially violative of the Fourth Amendment's protection against unreasonable searches and seizures.[4] D. 7 at 40-42; see D. 99 at 7 (noting that Plaintiffs argue that "every warrantless, suspicionless search of the *digital data* on an electronic device at the border violates the Fourth Amendment," with the exception of searches to verify that a laptop is operational and contains data). Defendants, in support of their own motion for summary judgment, argue that the border search exception to the Fourth Amendment's warrant requirement applies to both types of searches and no further showing is constitutionally required. D. 97 at 11-12.

[4] "[T]he distinction between facial and as-applied challenges is not so well defined that it has some automatic effect or that it must always control the pleadings and disposition in every case involving a constitutional challenge." Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 331 (2010); see City of Los Angeles, CA v. Patel, __ U.S. __, 135 S. Ct. 2443, 2449 (2015) (observing that while a facial challenge to a statute or governmental policy is "'the most difficult . . . to mount successfully,' the Court has never held that these claims cannot be brought under any otherwise enforceable provision of the Constitution" (internal citations omitted) (quoting United States v. Salerno, 481 U.S. 739, 745 (1987))).

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. "[A] warrantless search is *per se* unreasonable under the Fourth Amendment, unless one of 'a few specifically established and well-delineated exceptions' applies." United States v. Wurie, 728 F.3d 1, 3 (1st Cir. 2013) (quoting Arizona v. Gant, 556 U.S. 332, 338 (2009)). These few exceptions all arise from the exigent situations that "make the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment." Mincey v. Arizona, 437 U.S. 385, 393-94 (1978). These exceptions to the warrant requirement include exigent circumstances, searches incident to arrest, vehicle searches and, as relevant here, border searches. United States v. Cano, 934 F.3d 1002, 1011 (9th Cir. 2019) (citing Supreme Court precedent as to each exception).

1. Border Search Exception to the Warrant Requirement

The border search exception, "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," is one such exception. United States v. Ramsey, 431 U.S. 606, 620 (1977). As previously observed by this Court:

> [t]he border search serves the nation's "paramount interest in protecting[] its territorial integrity." Flores-Montano, 541 U.S. at 153. The rationales supporting the border search exception are the sovereign's interest in protecting the "integrity of the border," by "[r]egulat[ing] the collection of duties" and "prevent[ing] the introduction of contraband into this country." Montoya de Hernandez, 473 U.S. at 538, 537; see Carroll, 267 U.S. at 154 (explaining that "[t]ravellers may be so stopped . . . because of national self protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in"). The Supreme Court has characterized customs officials' role at the border as greater than that of "investigative law enforcement,"

> explaining that customs officers "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." Montoya de Hernandez, 473 U.S. at 544.

D. 34 at 39. The Court has further described such searches as extending to examinations of "persons and property crossing into this country," Ramsey, 431 U.S. at 616, to "prevent[] the entry of unwanted persons and effects" across the border, United States v. Flores-Montano, 541 U.S. 149, 152 (2004). "Absent more precise guidance from the founding era, we generally determine whether to exempt a given type of search exception from the warrant requirement 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" Riley v. California, 573 U.S. 373, 385 (2014) (citing Wyoming v. Houghton, 526 U.S. 295, 300 (1999)). That is, the border search exception is not limitless and must still be reasonable and subject to the same balancing of the level of intrusion upon an individual's privacy and its necessity for the promotion of legitimate governmental interests. D. 34 at 28-29 (citing United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985)).

What the border search exception recognizes, rather than a limitless ability to conduct searches in connection with international travel, is that individuals have a reduced expectation of privacy at the international border, while the government's "interest in preventing the entry of unwanted persons and effects is at its zenith" there. Flores-Montano, 541 U.S. at 152, 154. The balancing inquiry thus begins with the scales tipped heavily in favor of governmental interests.

2. Governmental Interests at the Border Are Paramount

Defendants have a paramount interest in maintaining "territorial integrity" at the border. They define such interest to include 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 D. 97 at 12 n.5 (citing 6 U.S.C. § 211); see 19 U.S.C. §§ 1461, 1496, 1582; 19 C.F.R. § 162.6. Defendants further cite the interests served by the border search exception as helping "to ensure national security; prevent the entry of criminals, inadmissible aliens, and contraband;" and to "facilitate[] lawful trade and travel." Id. To the extent that the government attempts to invoke "general law enforcement" purposes, that is not what gives rise to the border search exception, Cano, 934 F.3d at 1013, even as "the interdiction of contraband can serve both customs and law enforcement purposes." United States v. Smasal, No. Crim. 15-85 JRT/BRT, 2015 WL 4622246, at *10 (D. Minn. June 19, 2015) (Report and Recommendation). "No doubt a text message or email may reveal evidence of crimes, but that is true both at and inside the border. But it is uncertain whether the evidence-gathering justification is so much stronger at the border that it supports warrantless and suspicionless searches of the phones of the millions crossing it." United States v. Molina-Isidoro, 884 F.3d 287, 295 (5th Cir. 2018) (Costa, J., specially concurring). That is, as to contraband, it is the interdiction of contraband, not the mere evidence of contraband, that is a paramount concern at the border, not evidence of contraband that might be helpful in the investigations of past or future crimes. Cano, 934 F.3d at 1016-18 (recognizing "a difference between a search for contraband and a search for evidence of border-related crime," citing among other cases, Boyd v. United States, 116 U.S. 616, 622-23 (1886)); United States v. Vergara, 884 F.3d 1309, 1317 (11th Cir. 2018) (Pryor, J., dissenting) (noting that although "searching a cell phone may lead to the discovery of physical contraband," such a "general law enforcement justification is quite far removed from the purpose

originally underlying the border search exception: 'protecting this Nation from entrants who may bring anything harmful into this country'") (quoting Montoya de Hernandez, 473 U.S. at 544); D. 34 at 40 (citing Boyd, 116 U.S. at 623).

Otherwise, the Defendants' characterization of the government interests aligns with the Supreme Court's and Circuit courts' articulation of the rationale for the exception. Montoya de Hernandez, 473 U.S. at 544; see United States v. Soto-Soto, 598 F.2d 545, 549 (9th Cir. 1979) (noting that "Congress and the courts have specifically narrowed the border searches to searches conducted by customs officials in enforcement of customs laws"); United States v. Touset, 890 F.3d 1227, 1232 (11th Cir. 2018) (noting that "Congress has 'broad powers . . . to prevent smuggling and to prevent prohibited articles from entry' under its plenary authority '[t]o lay and collect Taxes, Duties, Imposts and Excises, [t]o regulate Commerce with foreign Nations,' and '[t]o establish a[ ] uniform Rule of Naturalization'") (internal citations omitted). That is, the "principal purposes" animating the border search exception are the government's interest in identifying "travellers . . . entitled to come in" and verifying their "belongings as effects which may be lawfully brought in." Cano, 934 F.3d at 1013 (quoting Carroll v. United States, 267 U.S. 132, 154 (1925)); D. 91-21 (CBP border search policy identifying the purpose of travelers' inspection "to ensure they are legally eligible to enter and that their belongings are not being introduced contrary to law"). Even as the governmental interests may be broader at the border, there still must be a showing of "the degree to which [the search exception] is needed for the promotion of legitimate governmental interests,'" Riley, 573 U.S. at 385, before weighing it against the degree of intrusion on an individual's privacy. United States v. Kim, 103 F. Supp. 3d 32, 57 (D.D.C. 2015) (noting that "[a]pplying the Riley framework, the national security concerns that underlie the enforcement of export control regulations at the border must be balanced against

the degree to which [the defendant's] privacy was invaded in this instance").

3. Even Border Searches Are Not Boundless

When applying exceptions to the warrant requirement, courts must determine whether the search at issue is within the scope of the exception, i.e., whether the search furthers the underlying purpose of the exception, and whether the search, even if within the scope of the exception, intrudes upon a competing privacy interest to such an extent that a warrant or other heightened level of suspicion should still be required. Riley, 573 U.S. at 386-401.

Undisputedly, interdiction of inadmissible persons and goods are legitimate governmental interests at the border. Plaintiffs do not dispute that CBP and ICE officers have the unenviable task of screening "[o]ver one million travelers per day [who] go through U.S. ports of entry," D. 99-1 at ¶ 14, and although they have some information about travelers (particularly those traveling by air and otherwise through agency databases), id. at ¶¶ 14, 20, they have little time to process it. See id. at ¶¶ 14, 22. Even so, the record that recites "searches of electronic devices at the border have successfully uncovered threats to national security, information pertaining to terrorism, illegal activities, contraband, and the inadmissibility of people and things," id. at ¶¶ 37, 50, without explanation of the frequency, nature of same or the manner of the discovery of same, is not a strong counterweight to the intrusion on personal privacy evidenced by such searches. Even assuming, as Defendants assert, that some such threats (or, for other examples, evidence of criminal conduct or contradictory information regarding a traveler's purpose for travel to the U.S., id. at ¶¶ 39-40) were uncovered in searches "without advance information or suspicion," id. at ¶ 38-40, on this record it is not clear that such would not be uncovered even when some cause, such as reasonable suspicion, could be developed (or has been developed in other cases as discussed below) in these

border encounters.[5] Further, the CBP and ICE policies contemplate relying on some cause for certain searches and actions at the border: i.e., reasonable suspicion for advanced searches of electronic devices; and as the CBP policy contemplates, probable cause for the "retention" of "an electronic device, or copies of information from the device" when "they determine that there is probable cause to believe that the device, or copy of the contents from the device, contains evidence of a violation of a law that CBP is authorized to enforce or administer," D. 91-18 at 9-10, even as this policy does not require such showing for "detention" of such devices "for a brief, reasonable period" or the retention of information relating to immigration, customs and other enforcement matters. Id.

As to the inadmissibility of travelers to the United States, the record is not clear as to what evidence of same would be revealed by a search of a traveler's electronic device. Although Defendants suggest that an electronic device may contain contradictory information about a traveler's stated purpose for visiting the United States, D. 99-1 at ¶ 39; D. 98-1 at ¶ 29, there is no suggestion that a search for same on the devices of the Plaintiffs would bear upon admission where ten of them are U.S. citizens and one is a lawful permanent resident of this country. D. 99-1 at ¶ 2 (acknowledging that U.S. citizens and lawful permanent residents are by definition admissible

[5] Moreover, the Court notes that the CBP policy as to the reasonable standard for advanced searches includes a "national security concern" exception. To the extent that such exception is akin to the well-recognized "exigent circumstances" exception to the warrant requirement, see D. 107 at 25-26, such exception would remain available regardless of the Court's ruling here. See Kentucky v. King, 563 U.S. 452, 460 (2011) (noting that this exception applies when "'the exigencies of the situation' make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment") (citing Mincey, 437 U.S. at 394); see also Riley, 573 U.S. at 402 (noting that exigent circumstances exception would still be available even as it ruled that a warrantless search of cell phone was not permissible as a search incident to arrest).

once identity and citizenship are established); cf. 8 U.S.C. § 1225 (providing that an alien who presents at the border "shall be deemed . . . an applicant for admission").

As to contraband, there are limits to the contraband that may be stored on digital devices. The forms of such contraband, as identified by Defendants, can include child pornography, classified information and counterfeit media, D. 98-1 at ¶¶ 23, 39; D. 99-1 at ¶¶ 35, 36, even as such devices may also contain evidence of contraband or other criminal or illegal conduct. D. 99-1 at ¶ 36. The record of the prevalence of such digital contraband encountered at the border remains unclear, even as to child pornography. D. 90-1 at 16 (noting that "[c]hild pornography, for instance, can be considered digital 'contraband' that may be interdicted at the border"); D. 97 at 23-24 n.6 (identifying cases involving searches that have uncovered contraband or evidence of illegality). Given the dearth of information of the prevalence of digital contraband entering the U.S. at the border, the Court cannot conclude that requiring a showing of some cause to search digital devices would obviate the deterrent effect of the border search exception. D. 99-1 at ¶ 47. "Notwithstanding the broad scope of the government's authority at the border, the Supreme Court has suggested that even this power to search may be bounded by limits derived from the Fourth Amendment, particularly when the search cannot be characterized as 'routine.'" Kim, 103 F. Supp. 3d at 49.

4. Border Search Exception Applies to Routine, Not Non-Routine Searches

The Supreme Court has described the border search exception as applying to "routine inspections and searches of individuals or conveyances seeking to cross our borders." Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973). "Routine searches of persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant." Montoya de Hernandez, 473 U.S. at 538. "Non-routine searches, by contrast, require reasonable

suspicion." Molina-Gomez, 781 F.3d at 19 (citing Montoya de Hernandez, 473 U.S. at 541-42). The distinction between routine and non-routine does not turn upon the frequency of such searches, or the label the government may ascribe to it, see Kim, 103 F. Supp. 3d at 55, but the degree of invasiveness or intrusiveness of the search. Molina-Gomez, 781 F.3d at 19 (citing United States v. Braks, 842 F.2d 509, 511-12 (1st Cir. 1988)). Although many of the factors for determining whether the degree of same makes a search routine or non-routine concern physical exposure or contact with the person being searched (e.g., whether search involved exposure of intimate body parts, physical contact between agents and person subject to search, whether search exposes person to pain or danger, Braks, 842 F.2d at 512), others do not necessarily (e.g., the overall manner in which search is conducted, even whether force was used and certainly "whether the suspect's reasonable expectations of privacy, if any, are abrogated by the search," id.). Even where the First Circuit in Braks concluded in 1988, long before the digital devices at issue here were available or commonplace, that the search of a defendant who lifted up her skirt to reveal a bulge in girdle that contained heroin was routine, id. at 513, it was careful to note that "[w]e do not suggest that the categorization of a border search as routine or non-routine can be accomplished merely by stacking up and comparing the several factors favoring each of the two classifications." Id. The court added that the factors above are not an "exhaustive list of equally-weighted concerns," but instead "[u]ltimately each case must turn upon its own particularized facts." Id.

That is, although as the court in Touset, 890 F.3d at 1234, noted, those border searches deemed non-routine have involved intrusive searches of a person, e.g., strip searches and body cavity searches, id. at 1235-38 (declining to conclude that any level of suspicion is constitutionally required for a search of electronic devices at the border, but, alternatively, finding that the agents had reasonable suspicion to search defendant's electronic devices); Molina-Gomez, 781 F.3d at 19

and cases cited; see Montoya de Hernandez, 473 U.S. at 541 (applying reasonable suspicion standard where traveler suspected of smuggling drugs ingested was subject to a physician's examination), does not mean that there are no searches of property that could constitute non-routine searches, particularly where they fall on the higher end of a continuum of invasiveness and intrusiveness than those routine searches that do not implicate such privacy concerns, like a pat-down, searching checked luggage, opening and testing bottles of liquor or removing and disassembling a gas tank. Molina-Gomez, 781 F.3d at 19 and cases cited.

There are a number of reasons and "a convincing case for categorizing forensic searches of digital devices as nonroutine": the "scale" and "sheer quantity" of personal information they contain, the "uniquely sensitive nature of that information," and the portable nature of same such that it is neither "'realistic nor reasonable to expect the average traveler to leave his digital devices at home when traveling.'" United States v. Kolsuz, 890 F.3d 133, 144-45 (4th Cir. 2018) (quoting United States v. Saboonchi, 990 F. Supp. 2d 536, 556 (D. Md. 2014)).

It is correct, as Defendants note, that no court has yet required a warrant for a search of an electronic device at the border. See, e.g., Kolsuz, 890 F.3d at 147 (noting that "there are no cases requiring more than reasonable suspicion for forensic cell phone searches at the border"); Vergara, 884 F.3d at 1311 (rejecting argument that border search of cell phones required a warrant or probable cause, but noting that "[a]t most, border searches require reasonable suspicion," which had not been argued by defendant); Molina-Isidoro, 884 F.3d at 292 (noting that "not a single court addressing border searches of computers since Riley has read it to require a warrant"); United States v. Wanjiku, 919 F.3d 472, 485 (7th Cir. 2019) (noting that "no circuit court, before or after Riley, has required more than reasonable suspicion for a border search of cell phones or electronically-stored data"). There is, however, growing precedent in the weighing of

governmental interests against privacy interests at the border of requiring a showing of reasonable suspicion at least for forensic searches of digital devices. For instance, in Molina-Gomez, the First Circuit declined to differentiate the search of the defendant's laptop and cell phones (X-rays of which were negative for contraband, inspection confirmed that they were operational, but on which agents reviewed inculpatory text messages), instead concluding that "even assuming the search was non-routine, reasonable suspicion existed to justify the search." Molina-Gomez, 781 F.3d at 20. The same was true, for another example, in Kolsuz, where the court ruled that "at least reasonable suspicion" was required, reasoning that "it is clear that a forensic search of a digital phone must be treated as a nonroutine border search, requiring some form of individualized suspicion." Kolsuz, 890 F.3d at 146.

5. Plaintiff's Privacy Interests in the Contents of their Electronic Devices

The privacy interest against which the Court must balance the justifications for the border search exception is an individual's interest in the contents of his or her electronic devices. The Court recognizes that while the "[g]overnment's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border," an individual's "expectation of privacy is less at the border than it is in the interior." Flores-Montano, 541 U.S. at 152, 154. Still, courts have recognized the "substantial personal privacy interests" implicated by the searches of electronic devices now "capable of storing warehouses full of information." United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013); see Riley, 573 U.S. at 393 (describing cell phones as "minicomputers that also happen to have the capacity to be used as a telephone"); Wurie, 728 F.3d at 9 (noting that "individuals today store much more personal information on their cell phones than could ever fit in a wallet, address book, briefcase, or any of the other traditional containers that the government has invoked"). This is true at the border as well. See Cotterman, 709 F.3d at

964; Kim, 103 F. Supp. 3d at 50 (noting that, given their "vast storage capacity" and capacity "to retain metadata and even deleted material, one cannot treat an electronic storage device like a handbag simply because you can put things in it and then carry it onto a plane"). The ICE and CBP policies cover the gamut of these electronic devices: the ICE policy defines electronic device as "[a]ny item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices," D. 98-4 at 3, and the CBP policy defines it as "[a]ny device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players," D. 98-5 at 3. Smart phones and laptops, devices that Plaintiffs were carrying, can contain information such as photographs, contact information, emails and text messages, as well as information such as prescriptions, employment information, travel history and internet browsing history. D. 99-1 at ¶ 64. Here, information on Plaintiffs' devices when the devices were searched includes attorney-client communications, D. 99-1 at ¶142, pictures of some Plaintiffs without their required religious attire, D. 99-1 at ¶¶ 122, 139, information related to Plaintiffs' journalism work, D. 99-1 at ¶ 129, and social media postings, D. 94 at 127-128. Even under the border search exception, it is the privacy interests implicated by unfettered access to such a trove of personal information that must be balanced against the promotion of paramount governmental interests at the border. Kim, 103 F. Supp. 3d at 55 (applying Riley).

It is in this balancing that the Supreme Court's ruling in Riley is particularly instructive. As explained at length in the earlier Memorandum & Order, the Court rejects Defendants' argument that Riley's reasoning should be limited to the search incident to arrest exception, not the matter at issue there. D. 34 at 28-46. The analysis in Riley carries persuasive weight in this

context, particularly where the Supreme Court has previously acknowledged that the search incident to arrest exception and the border search exceptions are "similar" as both are "longstanding, historically recognized exception[s] to the Fourth Amendment's general principle that a warrant be obtained." Ramsey, 431 U.S. at 621. Certainly, this Court is not alone in considering the analysis in Riley in resolution of a challenge to the application of the border search exception. See, e.g., Wanjiku, 919 F.3d at 484-85; Kolsuz, 890 F.3d at 140; Kim, 103 F. Supp. 3d at 54-58. In Riley, the Court analyzed the applicability of the search incident to arrest exception to searches of an arrestee's cell phone and held that officers must secure a warrant before conducting such a search. Riley, 573 U.S. at 386. The case was the consolidation of two cases below, both of which involved police examining an arrestee's phone subsequent to arrest, in one instance finding evidence of potential gang activity and in the other identifying the arrestee's home address and seeking a search warrant for the premises. Id. at 378-381. The Court examined the justifications for the search incident to arrest exception, namely, the risk of harm to officers from concealed material on an arrestee's person and the risk of destruction of evidence, and concluded that the justifications were untethered from searches of arrestees' cell phones. Id. at 388-391. Even taking into account the reduced privacy interest of an arrestee, the Court noted that "diminished privacy interests do[] not mean that the Fourth Amendment falls out of the picture entirely." Id. at 392. Riley further rejected the notion that searches of electronic devices are comparable to searches of physical items or persons, noting that such a comparison "is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." Riley, 573 U.S. at 393. The Supreme Court further noted later in the

opinion that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: [a] 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." Id. at 396-397 (emphasis in original). Riley, thus shows the challenge of applying and extending precedent concerning searches to new technology that presents a new privacy paradigm. See Carpenter v. United States, __ U.S.__, 138 S. Ct. 2206, 2222 (2018) (citing Riley, 573 U.S. at 386, ruling that the government must generally obtain a warrant to access cell phone location information and noting "[w]hen confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents"); United States v. Davis, 785 F.3d 498, 520 (11th Cir. 2015) (noting that "[j]udges cannot readily understand how . . . technologies may develop, cannot easily appreciate context, and often cannot even recognize whether the facts of the case before them raise privacy implications that happen to be typical or atypical") (citing Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L.Rev. 801, 858–59 (2004)); Morgan v. Fairfield Cty., Ohio, 903 F.3d 553, 575 n. 3 (6th Cir. 2018) (noting "how ever-changing technology fits within the contours of these zones may continue to challenge courts"). Riley also shows the vast privacy interests against which the promotion of governmental interests must be weighed.

It is the promotion of these governmental interests by the device searches under the border search exception where the record is sparser in support of Defendants' position. At the motion to dismiss stage, the Court noted that "the prevalence of physical transfers of illicit digital contraband across the U.S. borders (as opposed to through the internet) is unclear." D. 34 at 41. Defendants now cite thirty-four published cases involving seizure at the border of digital contraband or

evidence. D. 97 at 23 n.6. Even assuming that the thirty-four cases are not an exhaustive list of prosecutions resulting from border searches of electronic devices, as a percentage of all searches, this does not suggest a robust rate. CBP conducted approximately 108,000 searches of electronic devices at the border from fiscal year 2012 through fiscal year 2018. D. 90-2 at ¶ 52; D. 98 at ¶ 52. ICE does not track how many basic searches of electronic devices it conducts. D. 97 at 5. Comparing the thirty-four published cases cited by Defendants to the number of electronic devices searches performed by the CBP and over a shorter time frame than those published cases span, the number of searches that have led to seizures appears to be quite small.

Defendants also point to the broad latitude border officials have to search physical items, D. 104 at 7, but comparisons between searches for digital evidence or contraband and searches of other physical items or travelers themselves are inapposite. Riley recognized as much in responding to the government's argument that officers could search a cell phone if there were a sufficiently similar non-digital analogue that officers could have searched by noting that "the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years. And to make matters worse, such a test would allow law enforcement to search a range of items contained on a phone, even though people would be unlikely to carry such a variety of information in physical form." Riley, 573 U.S. at 400.

The Court's reasoning in Riley holds the same force when applied to border searches. Unlike a vehicle, vessel or even a home at the border, see 19 U.S.C. §§ 482, 1582, 1595(a)(2) (regarding inspections of vessels and homes), "the data stored on a cell phone is distinguished from physical records by quantity alone, [but] certain types of data are also qualitatively different."

Id. at 395-96. It can "reveal an individual's private interests or concerns" as evidenced by internet search and browsing history, "reveal where a person has been" through historic location information, and reveal which files a person created, accessed and when he or she did so through metadata. Id. The potential level of intrusion from a search of a person's electronic devices simply has no easy comparison to non-digital searches. See Cotterman, 709 F.3d at 966 (describing forensic search of digital device as "essentially a computer strip search").

6. The Broadly Defined Basic Search and Advanced Searches of Electronic Devices are Both Non-Routine Searches

Under the CBP and ICE policies, a basic search and an advanced search differ only in the equipment used to perform the search and certain types of data that may be accessed with that equipment, but otherwise both implicate the same privacy concerns. Basic searches, defined only as any search of an electronic device that is not an advanced search, can access content from space physically resident on a device using the devices' native operating system. D. 99-1 at ¶ 67. That is, even a basic search alone may reveal a wealth of personal information. Electronic devices carried by travelers, including smartphones and laptops, can contain a very large volume of information, including "sensitive information." D. 99-1 at ¶¶ 63, 65-66. Such devices can contain, for some examples, prescription information, information about employment, travel history and browsing history. D. 99-1 at ¶ 64. Such information can be accessed during not just the forensic searches under the CBP and ICE policies, but also under a basic search. D. 99-1 at ¶¶ 67-71. Using a device's native operating system, a basic search can access content from the allocated space physically present on the device, it can extend to any allocated file or information on the devices and, for devices that contain metadata, it can reveal "the date/time associated with the content, usage history, sender and receiver information or location data." D. 99-1 at ¶¶ 67-69. Even in a basic search, agents can peruse and search the contents of the device, using the native

search functions on the device, including, if available, a keyword search. D. 99-1 at ¶ 70. An agent conducting a basic search may use the device's own internal search tools to search for particular words or images. D. 99-1 at ¶ 71. Accordingly, even a basic search allows for both a general perusal and a particularized search of a traveler's personal data, images, files and even sensitive information.

This Court does not dispute that a cursory search of an electronic device—e.g., a brief look reserved to determining whether a device is owned by the person carrying it across the border, confirming that it is operational and that it contains data, D. 99 at 12—would fall within the border search exception and not require a heightened showing of cause. See, e.g., Cotterman, 709 F.3d at 960-61 (concluding that "a quick look and unintrusive search" of files on a laptop was a routine search, but a forensic search, "essentially a computer strip search" was nonroutine search requiring reasonable suspicion); Kim, 103 F. Supp. 3d at 57 (concluding that however the distinctions between a routine and forensic search are made by higher courts, the search at issue there was "qualitatively and quantitatively different from a routine border examination"). However, the range of searches that the Plaintiffs were subject to by CBP and ICE and the breadth of searches that continue to be permitted even as basic searches under the agencies' current policies, are not such routine searches given the breadth of intrusion into personal information.

The range of searches that Plaintiffs were subject to here illustrates this breadth. Although most were conducted before the current CBP and ICE policies were adopted on January 4, 2018 (CBP), D. 99-1 at ¶ 6, and May 11, 2018 (ICE), id. at ¶ 17, the record indicates that only a few of the searches of Plaintiffs' cellphones or laptops may have involved connection to external devices

and would have been characterized as advanced searches under the current policies,[6] while the others would have been considered basic searches (i.e., any search that is not an advanced search). These searches provided access to the photographs, contacts and data of both a personally and professionally sensitive nature. For one example, during one search of Dupin, a journalist, agents asked him about his phone's contents including photos, emails and contacts. D. 99-1 at ¶ 130; D. 91-4 at ¶ 8. CBP agents searched the phone of Shibly, a filmmaker and graduate student, D. 99-1 at ¶ 143, on two occasions, one for approximately thirty-seven minutes, D. 99-1 at ¶ 144; D. 91-8, and officers made notes of the contents. D. 94 at 128. Agents searched the cell phone of Bikkannavar, an optical engineer at NASA's Jet Propulsion Laboratory, D. 99-1 at ¶ 126, using what the CBP told him were "algorithms" to search his phone. D. 99-1 at ¶ 127; D. 91-3 at ¶ 12. Having had his phone searched by agents on several prior occasions, D. 99-1 at ¶ 134; D. 91-6, Kushkush, a freelance journalist, D. 99-1 at ¶ 133, had his phone taken by agents at the border and searched for an hour, D. 91-6 at ¶¶ 14-17, and then was questioned about his work as a journalist. His phone contained journalistic work product, work-related photos and lists of contacts. D. 91-6 at ¶ 8. These searches provided access to expressive content and personal contacts. For other examples, CBP agents searched the phone and laptop of Merchant, a writer, graduate student and founder and editor of a media website, D. 99-1 at ¶ 136. According to the uncontradicted attestation of Merchant, CBP officers asked her about one of her blog posts while searching her phone and laptop. D. 91-7 at ¶ 11. Her laptop and phone were taken out of her sight for one and

[6] As to one such search, on April 21, 2016, Wright had his phone, laptop and camera confiscated. D. 99-1 at ¶146. CBP "extracted and obtained information" from the devices, including attempting to image the laptop. D. 99-1 at ¶ 147. As to another, Allababidi, the owner and operator of a security technology business, had his phones, containing both personal and business information, searched for at least twenty minutes and then the agents detained the devices for a number of months for further examination, including having the phones sent to the "Regional Computer Forensic Lab." D. 99-1 at ¶¶ 124-25, 159; D. 91-2 at ¶ 4.

a half hours and when returned her phone was open to the Facebook friends page, which it had not been when she gave officers her phone. Id. at ¶ 13. The phone of Nadia Alasaad, a nursing student, D. 99-1 at ¶ 120, was searched despite her objections that it contained photographs of her and her daughters without the headscarf that they are required to wear in public in accordance with her religious beliefs. D. 91 at ¶ 10; D. 91-1 at ¶ 10. Both her phone and the phone of her husband, Ghassan Alasaad, a limousine driver, D. 99-1 at ¶ 120, were seized and not returned to them until fifteen days later. D. 91 at ¶ 18. Upon return, media files in one application, including videos of her daughter's graduation, indicated that they no longer existed on the phone and were not accessible. Id. at ¶ 19. Zorri, a university professor and former United States Air Force captain, D. 99-1 at ¶ 148, had her electronic devices, including her cell phone, searched for forty-five minutes, id. at ¶ 149.

Since the CBP and/or ICE adopted their search policies in 2018, the electronic devices of some Plaintiffs have also been searched in what were described as basic searches. For one example, on April 5, 2018, Merchant's phones were searched out of her sight for approximately forty-five minutes, D. 91-7 at ¶¶ 14-21, again on July 7, 2018, D. 91-7 at ¶¶ 22-24; D. 99-1 at ¶ 141; D. 91-7, and again on September 9, 2018. D. 91-7 at ¶¶ 26-32. On this last occasion, Merchant observed a CBP officer viewing emails and text messages between herself and her lawyer. Id. at ¶ 31; D. 99-1 at ¶ 142.

An advanced search can generally reveal anything that would be discovered during a basic search. D. 99-1 at ¶ 72. In addition to data revealed during a basic search, an advanced search also may be able to uncover deleted or encrypted data and copy all of the information physically present on the device depending on the equipment, procedures and techniques used. D. 99-1 at ¶¶ 73-74. Even if a device is not connected to the internet, if information from the internet is cached

on the device, agents can see and search the cached information. D. 99-1 at ¶ 75. That is, to the extent that the range of searches permissible as basic searches implicate privacy rights, so too as to the broader range of advanced searches.

On this record, and as Plaintiffs contend, D. 90-1 at 28; D. 107 at 11-12, the Court is unable to discern a meaningful difference between the two classes of searches in terms of the privacy interests implicated. The concerns laid out in Riley of unfettered access to thousands of pictures, location data and browsing history (which, applying the definition under the CBP and ICE policies would have qualified as a "basic search," Riley, 573 U.S. at 379-80), apply with equal force to basic and advanced searches, particularly as a device's native operating systems become more sophisticated and more closely mirror the capabilities of an advanced search. In light of this record, case law, and in conjunction with the lack of meaningful difference between basic and advanced searches, the Court concludes that agents and officials must have reasonable suspicion to conduct any search of entrants' electronic devices under the "basic" searches and "advanced" searches as now defined by the CBP and ICE policies. This requirement reflects both the important privacy interests involved in searching electronic devices and the Defendant's governmental interests at the border.

7. Reasonable Suspicion, not Probable Cause, Applies to Both Such Searches

Having not discerned a meaningful distinction between the currently defined basic search and advanced search in terms of privacy interests, reasonable suspicion should apply to both such searches at the border. Reasonable suspicion is a "common-sense conclusion[n] about human behavior upon which practical people,-including government officials, are entitled to rely." Montoya de Hernandez, 473 U.S. at 541-42 (quoting New Jersey v. T.L.O., 469 U.S. 325, 346 (1985)). Moreover, with a reasonable suspicion standard, "officials are afforded deference due to

their training and experience," Abidor v. Napolitano, 990 F. Supp. 2d 260, 282 (E.D.N.Y. 2013), and it allows authorities "'to graduate their response to the demands of any particular situation.'" Montoya de Hernandez, 473 U.S. at 542 (quoting United States v. Place, 462 U.S. 696, 709 n.10 (1983)). This standard is met when agents "can point to 'specific and articulable facts' . . . considered together with the rational inferences that can be drawn from those facts." Kim, 103 F. Supp. 3d at 43 (quoting Terry v. Ohio, 392 U.S. 1, 21, 30 (1968)).

The seeds of applying reasonable suspicion[7] in the border context have already been laid by several Circuits, post-Riley,[8] to the more intrusive searches of digital devices. See Kolsuz, 890 F.3d at 137; Cano, 934 F.3d at 1017; but see Touset, 890 F.3d at 1236 (concluding that "[w]e see

[7] Defendants argue that Plaintiffs have effectively waived any claim that reasonable suspicion should apply here, having not raised it as a separate claim in their complaint. D. 97 at 21; see D. 104 at 13. The Court rejects this argument. First, the Court has broad discretion to fashion appropriate remedies for constitutional violations. See Fed. R. Civ. P. 54(c), (providing that judgment "should grant the relief to which each party is entitled, even if the party has not demanded that relief in its pleadings"); see Town of Portsmouth, R.I. v. Lewis, 813 F.3d 54, 61 (1st Cir. 2016) (noting that a "plaintiff's failure to seek a remedy in its complaint does not necessarily forego that remedy"). Second, Plaintiffs have sought broad relief, including "such other and further relief as the Court deems proper" and have consistently argued, since at least the motion to dismiss stage, that reasonable suspicion would be an alternative remedy to a probable cause standard and thus Defendants have been on notice of the possible relief, D. 99 at 8-9. Third, courts analyzing the issue of warrantless searches of electronic devices at the border have noted that review "necessarily encompasses a determination as to the applicable standard: no suspicion, reasonable suspicion of probable cause" and found no prejudice in analyzing the reasonable suspicion standard even when not fully briefed on appeal. See Cotterman, 709 F. 3d at 960. There is also no prejudice to Defendants in considering this issue as the reasonable suspicion standard, in addition to being a part of Defendants' present policies with respect to advanced searches of electronic devices, has been repeatedly discussed in the parties' briefing, see, e.g., D. 15 at 24; D. 19 at 24, as well as in the Court's Memorandum & Order on the motion to dismiss, D. 34 at 44.

[8] Some such seeds came pre-Riley. See Cotterman, 709 F.3d at 968 (concluding that "the forensic examination of Cotterman's computer required a showing of reasonable suspicion, a modest requirement in light of the Fourth Amendment"); Abidor, 990 F. Supp. 2d at 280-82 (noting that "[a] comprehensive forensic search of a computer, whether a desktop or a laptop, involves a significant invasion of privacy" and that "if suspicionless forensic computer searches at the border threaten to become the norm, then some threshold showing of reasonable suspicion should be required").

no reason why we would permit traditional, invasive searches of all other kinds of property but create a special rule that will benefit offenders who now conceal contraband in a new kind of property") (internal citation omitted).

Moreover, the reasonable suspicion that is required for the currently defined basic search and advanced search is a showing of specific and articulable facts, considered with reasonable inferences drawn from those facts, that the electronic devices contains contraband. Although this may be "a close question" on which at least two Circuits disagree, Cano, 934 F.3d at 1017-18 (noting its disagreement with the Fourth Circuit in Kolsuz, 890 F.3d at 143, on this point), the Court agrees that this formulation is consistent with the government's interest in stopping contraband at the border and the long-standing distinction that the Supreme Court has made between the search for contraband, a paramount interest at the border, and the search of evidence of past or future crimes at the border, which is a general law enforcement interest not unique to the border. See Cano, 934 F.3d at 1018-20 (citing Boyd, 116 U.S. 616, 622-23 and concluding that border search exception authorizes warrantless searches of a cell phone only for contraband and that "border officials may conduct a forensic cell phone search only when they reasonably suspect that the cell phone contains contraband"). Although Defendants have the twin interests of protecting territorial integrity by preventing the entry of both contraband and inadmissible persons, this record does not reveal what, if any, evidence would be contained on the electronic devices, particularly of Plaintiffs, all U.S. citizens and one lawful resident alien, that would prevent their admission. Even as to an alien, where CBP posits that an electronic device might contain contradictory information about his/her intentions to work in the U.S. contrary to the limitations of a visa, D. 98-1 at ¶ 29, there is no indication as to the frequency of same or the necessity of unfettered access to the trove of personal information on electronic devices for this purpose. See

Riley, 573 U.S. at 398-99 (rejecting extension of the Gant standard for warrantless vehicle searches to cell phones given the breadth of data, unrelated to any present crime, that a cell phone could provide such that application of the standard to cell phones "would in effect give "'police officers unbridled discretion to rummage at will among a person's private effects'") (internal citation omitted). Moreover, this standard focused on discovery of contraband reflects the judicial preference "to provide clear guidance to law enforcement through categorical rules." Riley, 573 U.S. at 399.

Even if the CBP's and ICE's adoption of a reasonable suspicion standard for advanced searches is not a concession that such standard is constitutionally required, it is at least an acknowledgment that the legal tide is turning in this direction and, more importantly, that even border searches may lend themselves to such showing. In January 2018, CBP revised its directive concerning border searches of electronic devices to make a distinction between basic and advanced searches and to require reasonable suspicion or a national security concern for an advanced search. D. 99-1 at ¶ 7. CBP officers have procedures for conducting advanced searches of electronic devices based on reasonable suspicion. D. 90-2 at ¶ 116. ICE agents use the same definitions of basic and advanced searches as CBP and ICE policy is to only conduct advanced searches when there is reasonable suspicion, D. 99-1 at ¶ 9; see also D. 98-2 at ¶ 12. Both agencies provide training on the reasonable suspicion standard, D. 90-2 at ¶ 118, and border agents have experience with applying this standard. D. 91-12 at 79-80.

The same is true where courts have not necessarily required reasonable suspicion for searches of electronic devices at the border but concluded this standard had been met by the agents in a particular case. Wanjiku, 919 F.3d at 488-489 (holding that customs agents had good faith belief that warrantless border search of electronic devices did not violate the Fourth Amendment

and that search was supported by reasonable suspicion); Touset, 890 F.3d at 1237 (concluding, alternatively, that agents had reasonable suspicion to search the defendant's electronic devices); Molina-Isidoro, 884 F.3d at 289 (declining to announce general rules with respect to border searches and electronic devices because search was supported by probable cause); Molina-Gomez, 781 F.3d at 19-20 (declining to determine whether search was non-routine or routine, but noting that reasonable suspicion standard for non-routine search had been met); Abidor, 990 F. Supp. 2d at 283 (concluding that "agents certainly had reasonable suspicion supporting further inspection of Abidor's electronic devices"); United States v. Hampe, No. 07-3-B-W, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007) (concluding that "even if the Court were to entertain the proposition that reasonable suspicion is required to search a computer at the border, the peculiar facts presented to the officers in this case gave rise to a reasonable suspicion"). Most of these cases, although not all, involved electronic devices that contained contraband (as opposed to evidence of contraband). Wanjiku, 919 F.3d at 477-78 (child pornography); Touset, 890 F.3d at 1237 (same); Molina-Gomez, 781 F.3d at 17 (laptop and Playstation contained hides of heroin); Hampe, 2007 WL 1192365, at *4 (child pornography). The same is true of more than half of the broader array of published cases cited by Defendants, some of which were issued prior to Riley, D. 97 at 23 n.6. Although the Court understands Defendants' contention that it might be impracticable to require a warrant for all searches of electronic devices at the border, D. 99-1 at ¶¶ 43, 45, 48, impracticability is not the touchstone for the legal analysis here, rather the touchstone is reasonableness. Riley, 573 U.S. at 381 (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)). Moreover, impracticality lessens where the cause required here is that of an investigatory stop, that need not be known in advance, but where CBP and ICE agents have the "emerging tableau" of primary and secondary inspections to determine if reasonable suspicion exists for the search of electronic

devices for contraband. United States v. Chhien, 266 F.3d 1, 6 (1st Cir. 2001) (addressing reasonable suspicion for an investigative stop which, justified at the inception, must also reveal that "the officer's subsequent actions were fairly responsive to the emerging tableau—the circumstances originally warranting the stop, informed by what occurred, and what the officer learned, as the stop progressed"). It is this emerging tableau that the agents will be responding to (and for which they are already implementing and preparing to implement as to advanced searches), and which agents have already done as reflected in the border search cases referenced above.

Although the border search exception and the search incident to arrest exception are similar, narrow exceptions to the search warrant requirement, the Court recognizes the governmental interests are different at the border and holds that reasonable suspicion and not the heightened warrant requirement supported by probable cause that Plaintiffs seek here and as applied to the search in Riley is warranted here. Accordingly, the Court ALLOWS IN PART Plaintiffs' motion for summary judgment as to Count I and DENIES Defendants' motion for summary judgment as to this Count.

C. Plaintiffs' First Amendment Claim (Count II)

Plaintiffs, in addition to their Fourth Amendment claims, argue that the First Amendment's protections require border agents to seek a warrant before searching travelers' electronic devices. Plaintiffs' argument relies on the uncontested fact that the contents of electronic devices include "highly sensitive information concerning Plaintiffs' personal, privileged, confidential, and anonymous communications and associations." D. 90-1 at 23. The parties also agree that such information and materials constitute or include expressive materials that implicate First Amendment issues. D. 90-1 at 23; D. 97 at 23-24.

The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble." U.S. Const. amend. I. As the Court noted in ruling on the motion to dismiss, these rights "are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference." D. 34 at 47 (citing Bates v. City of Little Rock, 361 U.S. 516, 523 (1960)). For instance, "associational rights . . . can be abridged even by government actions that do not directly restrict individuals' ability to associate freely." Lyng v. Int'l Union, UAW, 485 U.S. 360, 367 n.5 (1988); see AFL-CIO v. FEC, 333 F.3d 168, 175 (D.C. Cir. 2003) (explaining that compulsory "disclosure of political affiliations and activities can impose just as substantial a burden on First Amendment rights as can direct regulation"); Baird v. State Bar of Ariz., 401 U.S. 1, 6-7 (1971) (explaining that "[w]hen a State seeks to inquire about an individual's beliefs and associations a heavy burden lies upon it to show that the inquiry is necessary to protect a legitimate state interest").

The parties disagree on the appropriate standard for balancing governmental interest in the border searches of electronic devices against travelers' First Amendment freedoms. D. 90-1 at 23; D. 97 at 25. The first question for such analysis is whether the border searches of electronic devices of Plaintiffs and under the CBP and ICE policies burden those freedoms at all. See, e.g., McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342-45 (1995); Boy Scouts of Am. v. Dale, 530 U.S. 640, 657–59 (2000). As the Court noted at the motion to dismiss stage, the policies at issue here are content-neutral. D. 34 at 48. Compelled disclosure of First Amendment protected activity, however, can itself be a burden. See Buckley v. Valeo, 424 U.S. 1, 64 (1976). Where such burden is present, as an "inevitable result of the government's conduct in requiring disclosure," there must be a "substantial relation between the governmental interest and the information required to be

disclosed." Id. at 64-65. Stated otherwise, "an infringement on [First Amendment] rights is not unconstitutional so long as it 'serve[s] compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through means significantly less restrictive of associational freedoms.'" Tabbaa, 509 F.3d at 102 (quoting Roberts v. United States Jaycees, 468 U.S. 609, 623 (1984)); cf. House v. Napolitano, 2012 WL 1038816, at *2, *13 (declining to dismiss First Amendment claim particularly given the allegations in the complaint that plaintiff was targeted and investigated because of his associations and the search of his laptop resulted in disclosure of same). Although it remains correct that an encounter at the border "does not strip [a citizen] of his First Amendment rights," House, 2012 WL 1038816, at *13, here, where the paramount government interests are the interdiction of persons and goods at the border, and there is no suggestion on this developed record that Plaintiffs were targeted and investigated for their speech or associations as the plaintiff in House alleged, it is not clear what less restrictive means could be employed here. This is particularly true where the Court adopts a standard requiring that any such searches be conducted with reasonable suspicion that the electronic devices contain contraband, which is not protected speech. See New York v. Ferber, 458 U.S. 747, 763 (1982) (concluding that child pornography is not protected by the First Amendment). That is, any burden on First Amendment rights from the border agents' viewing of any expressive materials is inextricably tied to, and therefore substantially related to, when supported by reasonable suspicion, a non-cursory searching of a traveler's electronic devices at the border.

Although Ramsey, 431 U.S. at 624, involved Fourth Amendment and First Amendment issues, the Court's ruling resolved the Fourth Amendment issue, holding that customs and border officers could search international mail where suspicion of contraband was present but "hav[ing] no occasion to decide whether, in the absence of the regulatory restrictions [prohibiting the reading

of expressive material within the mail], speech would be 'chilled,' or, if it were, whether the appropriate response would be to apply the full panoply of Fourth Amendment requirements." Id. at n.18. Although Ramsay did not squarely resolve the issue, a different standard for First Amendment issues from the Fourth Amendment issues is not necessarily required. United States v. Brunette, 256 F.3d 14, 16 (1st Cir. 2001) (analyzing probable cause for a search warrant for child pornography, i.e., whether there was a 'fair probability that contraband or evidence of a crime would be found in a particular place,' and concluding that "assessments [are] no different where First Amendment concerns may be at issue") (internal citation omitted); see New York v. P.J. Video, Inc., 475 U.S. 868, 875 (1986) (noting "that an application for a warrant authorizing the seizure of materials presumptively protected by the First Amendment should be evaluated under the same standard of probable cause used to review warrant applications generally"). This is even true as the Court considers searches at the border.

Accordingly, to the extent that Count II seeks some further ruling or relief based upon Plaintiffs' invocation of First Amendment rights, not otherwise granted as to Count I, the Court DENIES Plaintiffs' motion for summary judgment and DENIES Defendants' motion for summary judgment as to Count II.

D. Plaintiffs' Seizure of Electronic Devices Claim (Count III)

Certain of Plaintiffs claim that the government's seizure of their electronic devices with the intent to search the devices after they left the border violated the Fourth Amendment due to a lack of probable cause (the same level of suspicion Plaintiffs contend should be required for a search of the devices) for the seizure at the time it was made. See Kolsuz, 890 F.3d at 141 (noting that, with respect to confiscation of an electronic device, "a seizure reasonable at its inception must remain reasonable in scope and duration to satisfy the Fourth Amendment"); Molina-Gomez, 781

F.3d at 21 (applying same analysis to both search of defendant's electronic devices and seizure of same). As the Court has previously noted, this claim is not coterminous with Count I since prolonged detention of electronic devices that may have been reasonable at their inception can become unreasonable. D. 34 at 46 and cases cited. The touchstone for any such detention remains reasonableness. Place, 462 U.S. at 709 (declining to adopt any outside time limitation for a Terry stop but concluding that the 90-minute detention of respondent's luggage was sufficient to render the seizure unreasonable under the Fourth Amendment). Although the seizure in Place was not at the border, some inquiry into the reasonableness of the duration of a seizure at the border remains appropriate. Given the border context, the Supreme Court has been reluctant to adopt "hard-and-fast time limits" for the reasonableness of detention. Montoya de Hernandez, 473 U.S. at 543 (citing Place, 462 at 709 n.10 and other cases). The Court is reluctant to do so here on this record, given the current CBP and ICE policies regarding same and in light of its ruling as to the reasonable suspicion requirement for non-cursory border searches of electronic devices except as follows. Where border agents seize an electronic device for non-cursory search supported by reasonable suspicion, such detention must be for a reasonable period that allows for an investigatory search for contraband. See D. 91-18 (CBP policy making a distinction between "detention" of electronic devices for "a brief, reasonable period of time" not requiring cause and "retention" of such devices or information from such devices requiring probable cause to believe they contain "evidence of a violation of law that CBP is authorized to enforce or administer" unless the information retained relates to immigration, customs and "other enforcement matters").

Accordingly, the Court ALLOWS IN PART Plaintiffs' motion for summary judgment as to Count III to the extent that it seeks the ruling above and DENIES Defendants' motion for summary judgment as to same.

E. Relief Sought

1. Expungement Not Warranted Here

As part of the relief sought, Plaintiffs seek expungement of all information gathered from, or copies made of, the contents of Plaintiffs' electronic devices including social media information and device passwords. As addressed in the discussion of Plaintiffs' standing, the Court understands that Plaintiffs seek such relief, at least in part, since previous border searches may lead to future border searches under the agencies' policies. See Section V(A), *supra.* That is, as this Court previously held, Plaintiffs have plausibly alleged that expungement would afford them some redress as to their claims. D. 34 at 26. Still, expungement is an extraordinary measure committed to the discretion of the Court. Sealed Appellant v. Sealed Appellee, 130 F.3d 695, 701 (5th Cir. 1997) (reversing an order commanding executive branch agencies to expunge the records of a defendant's now overturned convictions); Chastain v. Kelley, 510 F.2d 1232, 1236 (D.C. Cir. 1975) (noting that "[e]xpungement, no less than any other equitable remedy, is one over which the trial court exercises considerable discretion," but vacating order of expungement).

Although this is not a criminal case, considering the remedy for the unconstitutional search in the criminal context is illustrative of the extraordinary nature of the remedy sought here. Even where law enforcement officers have conducted a search in violation of the Constitution, the "fruits of [the] search need not be suppressed if the agents acted with the objectively reasonable belief that their actions did not violate the Fourth Amendment." Molina-Isidoro, 884 F.3d at 290 (applying the good faith exception under United States v. Leon, 468 U.S. 897 (1984) to the exclusionary rule to agents' warrantless search of the defendant's phone at the border). "In such circumstances, the cost of suppression—excluding the evidence from the truth-finding process—outweighs the deterrent effect suppression may have on police conduct." Molina-Isidoro, 884 F.3d

at 290; see Pennsylvania Bd. of Probation and Parole v. Scott, 524 U.S. 357, 363 (1998) (noting that because the exclusionary rule "is prudential rather than constitutionally mandated, we have held it to be applicable only where its deterrence benefits outweigh its 'substantial social costs'"). Even where suppression is warranted, the remedial measure is that the fruits of the search cannot be used against the subject of the search in a criminal trial, not some further form of exclusion of these fruits. Scott, 524 U.S. at 363-64 (noting that it has "repeatedly declined to extend the exclusionary rule to proceedings other than criminal trials" and holding that the exclusionary rule "does not bar the introduction at parole revocation hearings of evidence seized in violation of parolees' Fourth Amendment rights"); Immigration and Naturalization Serv. v. Lopez-Mendoza, 468 U.S. 1032, 1050 (1984) (weighing the deterrent value against the social costs and declining to apply the exclusionary rule in civil deportation hearings). If the costs of exclusion are too high in criminal trials where agents have a good faith basis for believing a search did not violate the Fourth Amendment, at least the same must be true at the border given the paramount governmental interests previously discussed, particularly where the law regarding the legality of electronic device searches has been in flux and has been the subject matter of ongoing litigation in several courts.

The same is also true of the analogous, but broader, remedy of expungement of the information obtained during searches of Plaintiffs' electronic devices. Even where evidence obtained in an unconstitutional manner has been suppressed, a further remedy of expungement does not follow. See United States v. Fields, 756 F.3d 911, 917 (6th Cir. 2014) (declining to expunge arrest record where evidence was suppressed and such remedy was not necessary "to vindicate" the trial court's rulings or the suppression remedy). That is, even where criminal proceedings followed a border search that exceeded the bounds of the Fourth Amendment and the

fruits of same were suppressed, expungement of the border agents' files would not necessarily follow. Nor should it where other deterrents to border agents' unconstitutional searches remain in place. Such measures include, but are not limited to, the possibility of declaratory relief against the agency, training of border agents regarding constitutional requirements for searches, see Lopez-Mendoza, 468 U.S. at 1046 (citing, among other things, the instruction and examination in Fourth Amendment law that officers receive in concluding that deterrent effect of exclusionary rule would be met by other measures); see D. 99-1 at ¶¶ 105 (noting that CBP officers receive written guidance and training on what constitutes probable cause and how to obtain warrants), 111-112 (same regarding ICE agents), 118 (undisputed that both CBP and ICE officers receive training on reasonable suspicion); D. 91-26 at 3 (CBP accepting recommendations of Office of Inspector General audit of agency's border searches of electronic devices), disciplinary action or other consequences against agents who violate agency policies complying with the law, see 91-28 at 6, and "because application of the [exclusionary] rule in the criminal trial context already provides significant deterrence of unconstitutional searches." Scott, 524 U.S. at 364.

Putting aside the balancing of the deterrent effect on border agents that expungement of this information may have, Plaintiffs seek expungement also to protect them from the future harm of more likely being subject to border searches. In the civil context, a court in its discretion may order expungement for the purposes of remedying ongoing or future harm where such "is an equitable remedy designed to correct, not compensate for, the violation, and may be essential to prevent future harm as a result of the original violation." Carter v. Orleans Parish Pub. Schs., 725 F.2d 261, 263 (5th Cir. 1984) (dismissing claim for expungement in the absence of an allegation that defendant school continues to maintain records falsely characterizing the children as "mentally retarded"); see Bruso v. United Airlines, Inc., 239 F.3d 848, 863 (7th Cir. 2001) (noting that "[a]

court may use expungement as a means of removing the stain of the employer's discriminatory actions from the plaintiff's permanent work history). Still, the Court, in its discretion, must determine if such remedy is necessary, particularly where the Court is granting other forms of relief, namely, the measures noted above that may have a deterrent effect and the ruling that reasonable suspicion is required for basic and advanced searches. That is, in the future, whether information has been retained from prior searches or not, agents must be able to point to specific and articulable facts for reasonable suspicion to believe that Plaintiffs' electronic devices contain contraband, which also addresses the concern about any likelihood, greater than the general public of U.S. citizens returning to the U.S. borders, of being subject to a non-cursory search. In light of this other relief, including declaratory relief, the Court DENIES the request for expungement of information[9] taken from their digital devices given the declaratory relief provided below and ruling that reasonable suspicion is required for the basic and advanced searches.

2. Extent of Declaratory and Injunctive Relief

As to declaratory relief, Plaintiffs seek: a) declaration that Defendants' policies violate the First and Fourth Amendment facially and have violated Plaintiffs' First and Fourth Amendment rights by authorizing and conducting searches of electronic devices absent a warrant supported by probable cause, D. 7 at 40-41 ¶¶ A-B; and b) declarations that Defendants' policies violate the Fourth Amendment facially and have violated Plaintiffs' Fourth Amendment rights by authorizing and conducting the confiscation of electronic devices absent probable cause, id. at 41 ¶¶ D-F. The Court grants this relief, but only to the extent consistent with its ruling here. Accordingly, the Court ALLOWS the request for declaratory relief to the following extent: the Court declares that

[9] To the extent that Plaintiffs were also seeking expungement of passcodes or other means of access, the CBP policy provides for destruction of same, D. 91-18 at 7, and there is no indication in the record that such information has been retained.

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

As to injunctive relief, Plaintiffs seek: a) an injunction preventing Defendants from "searching electronic devices absent a warrant supported by probable cause that the devices contain contraband or evidence of a violation of immigration or customs laws," id. at 41 ¶ C; and b) an injunction preventing Defendants from confiscating electronic devices, with the intent to search the devices after the travelers leave the border, without probable cause and without promptly seeking a warrant for the search, id. at 41 ¶ G. Although there has been extensive briefing by both sides in this case, the bulk of that briefing focused on Plaintiffs' standing to bring their claims and the merits of those claims and not the scope of the relief, particularly the scope of injunctive relief, sought by Plaintiffs. D. 90-1, 97, 99, 104. Given that Plaintiffs reside across the United States and Canada, were searched at different border entries and that the Plaintiffs sought a facial challenge to the constitutionality of such searches, it may be that Plaintiffs seek injunctive relief on a nationwide basis. Even if the Court had applied the warrant supported by probable cause standard reflected in Plaintiffs' request for injunctive relief, the Court would not have imposed nationwide or universal injunction without further briefing from the parties. See Trump v. Hawaii, __ U.S. __, 138 S. Ct. 2392, 2424 (2018) (Thomas, J., concurring); Washington v. Trump, 847 F.3d 1151, 1169 (9th Cir. 2017) (per curiam) (affirming nationwide injunction of the Trump Administration's travel ban); City of Chicago v. Sessions, 888 F.3d 272, 288 (7th Cir. 2018) (affirming nationwide injunction of the Trump Administration's withholding of federal

funds from "sanctuary cities"); Texas v. United States, 787 F.3d 733, 768-69 (5th Cir. 2015) (affirming nationwide injunction of Deferred Action for Parents of Americans); Texas v. United States, No. 1:18-CV-00068, 2018 WL4178970, at *61-62 (Aug. 31, 2018) (declining to issue nationwide preliminary injunction halting Deferred Action for Childhood Arrivals program); Compare Samuel L. Bray, Multiple Chancellors: Reforming the National Injunction, 131 Harv. L. Rev. 417, 418 (2017) (concluding nationwide injunctions encourage forum shopping, hurt judicial decisionmaking and create risk of conflicting injunctions) with Amanda Frost, In Defense of Nationwide Injunctions, 93 N.Y.U. L. Rev. 1065 (2018) (concluding nationwide injunctions are not barred by statute nor the Constitution and "enable federal courts to play their essential role as a check on the political branches"). Accordingly, the Court DENIES the request for injunctive relief without prejudice.

VI. Conclusion

For the foregoing reasons, the Court ALLOWS IN PART and DENIES IN PART Plaintiffs' motion for summary judgment, D. 90 and DENIES Defendants' motion for summary judgment, D. 96.

So Ordered.

/s/ Denise J. Casper
United States District Judge

UNITED STATES DISTRICT COURT
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 ZORRI, 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.**	**No. 17-cv-11730-DJC**

JUDGMENT

CASPER, J. **November 21, 2019**

Having considered the parties' Joint Statement Regarding Relief, D. 111, and in light of the Court's Memorandum and Order regarding the parties' motions for summary judgment, D. 109, the Court enters judgment as follows:

1. Having allowed in part and denied in part Plaintiffs' motion for summary judgment, D. 90, and denied Defendants' motion for summary judgment, D. 96, the Court enters

judgment for Plaintiffs to that extent as explained in the Court's Memorandum and Order, D. 109;

2. As to the declaratory relief Plaintiffs seek, D. 111 at 1, and consistent with the Court's Memorandum and Order, D. 109 at 46-47, the Court grants declaratory judgment as follows:

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

3. As to the injunctive relief Plaintiffs seek, D. 111 at 1-4, the Court concludes that Plaintiffs, on this record, have satisfied the legal standard for the injunctive relief they seek, id. at 2, where Plaintiffs have prevailed on the merits, Plaintiffs would suffer irreparable harm in the absence of the injunctive relief they seek, the balance of harms between the parties weighs in favor of granting the injunctive relief sought and the public interest weighs in favor of such relief as well, id. at 2-4, and, accordingly, the Court:

> enjoins Defendants from searching or seizing any electronic device belonging to a Plaintiff during any encounter with a Plaintiff at the border or functional equivalent of the border, unless Defendants have reasonable suspicion that the device contains contraband. Should Defendants conduct any search or seizure of a Plaintiff's electronic device at the border based on reasonable suspicion that the device contains contraband, the Court further enjoins Defendants from detaining the device longer than a reasonable period that allows for an investigatory search for that contraband.

So Ordered.

/s/ Denise J. Casper
United States District Judge

U.S. CUSTOMS AND BORDER PROTECTION

CBP DIRECTIVE NO. 3340-049A

DATE: January 4, 2018
ORIGINATING OFFICE: FO:TO
SUPERSEDES: Directive 3340-049
REVIEW DATE: January 2021

SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES

1 **PURPOSE.** To provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, tablets, removable media, disks, drives, tapes, mobile phones, cameras, music and other media players, and any other communication, electronic, or digital devices subject to inbound and outbound border searches by U.S. Customs and Border Protection (CBP). These searches are conducted in furtherance of CBP's customs, immigration, law enforcement, and homeland security responsibilities and to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer.

These searches are part of CBP's longstanding practice and are essential to enforcing the law at the U.S. border and to protecting border security. They help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark, and export control violations. They can be vital to risk assessments that otherwise may be predicated on limited or no advance information about a given traveler or item, and they can enhance critical information sharing with, and feedback from, elements of the federal government responsible for analyzing terrorist threat information. Finally, searches at the border are often integral to a determination of an individual's intentions upon entry and provide additional information relevant to admissibility under the immigration laws.

2 **POLICY**

2.1 CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission.

2.2 All CBP Officers, Border Patrol Agents, Air and Marine Agents, Office of Professional Responsibility Agents, and other officials authorized by CBP to perform border searches shall adhere to the policy described in this Directive and any implementing policy memoranda or musters.

2.3 This Directive governs border searches of electronic devices – including any inbound or outbound search pursuant to longstanding border search authority and conducted at the physical border, the functional equivalent of the border, or the extended border, consistent with law and agency policy. For purposes of this Directive, this excludes actions taken to determine if a device functions (e.g., turning a device on and off); or actions taken to determine if physical contraband is concealed within the device itself; or the review of information voluntarily provided by an individual in an electronic format (e.g., when an individual shows an e-ticket on an electronic device to an Officer, or when an alien proffers information to establish admissibility). This Directive does not limit CBP's authority to conduct other lawful searches of electronic devices, such as those performed pursuant to a warrant, consent, or abandonment, or in response to exigent circumstances; it does not limit CBP's ability to record impressions relating to border encounters; it does not restrict the dissemination of information as required by applicable statutes and Executive Orders.

2.4 This Directive does not govern searches of shipments containing commercial quantities of electronic devices (e.g., an importation of hundreds of laptop computers transiting from the factory to the distributor).

2.5 This Directive does not supersede *Restrictions on Importation of Seditious Matter*, Directive 2210-001A. Seditious materials encountered through a border search should continue to be handled pursuant to Directive 2210-001A or any successor thereto.

2.6 This Directive does not supersede *Processing Foreign Diplomatic and Consular Officials*, Directive 3340-032. Diplomatic and consular officials encountered at the border, the functional equivalent of the border (FEB), or extended border should continue to be processed pursuant to Directive 3340-032 or any successor thereto.

2.7 This Directive applies to searches performed by or at the request of CBP. With respect to searches performed by U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) Special Agents exercise concurrently-held border search authority that is covered by ICE's own policy and procedures. When CBP detains, seizes, or retains electronic devices, or copies of information therefrom, and conveys such to ICE for analysis, investigation, and disposition (with appropriate documentation), the conveyance to ICE is not limited by the terms of this Directive, and ICE policy will apply upon receipt by ICE.

3 DEFINITIONS

3.1 Officer. A Customs and Border Protection Officer, Border Patrol Agent, Air and Marine Agent, Office of Professional Responsibility Special Agent, or any other official of CBP authorized to conduct border searches.

3.2 Electronic Device. Any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players.

3.3 Destruction. For electronic records, destruction is deleting, overwriting, or degaussing in compliance with CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05C.

4 AUTHORITY/REFERENCES. 6 U.S.C. §§ 122, 202, 211; 8 U.S.C. §§ 1225, 1357, and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. § 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. § 401 and other laws relating to exports; Guidelines for Detention and Seizures of Pornographic Materials, Directive 4410-001B; Disclosure of Business Confidential Information to Third Parties, Directive 1450-015; Accountability and Control of Custody Receipt for Detained and Seized Property (CF6051), Directive 5240-005.

The plenary authority of the Federal Government to conduct searches and inspections of persons and merchandise crossing our nation's borders is well-established and extensive; control of the border is a fundamental principle of sovereignty. "[T]he United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). "The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Time and again, [the Supreme Court has] stated that 'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.'" *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)). "Routine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). Additionally, the authority to conduct border searches extends not only to persons and merchandise entering the United States, but applies equally to those departing the country. *See, e.g.*, *United States v. Boumelhem*, 339 F.3d 414, 422-23 (6th Cir. 2003); *United States v. Odutayo*, 406 F.3d 386, 391-92 (5th Cir. 2005); *United States v. Oriakhi*, 57 F.3d 1290, 1296-97 (4th Cir. 1995); *United States v. Ezeiruaku*, 936 F.2d 136, 143 (3d Cir. 1991); *United States v. Cardona*, 769 F.2d 625, 629 (9th Cir. 1985); *United States v. Udofot*, 711 F.2d 831, 839-40 (8th Cir. 1983).

As a constitutional matter, border search authority is premised in part on a reduced expectation of privacy associated with international travel. *See Flores-Montano*, 541 U.S. at 154 (noting that "the expectation of privacy is less at the border than it is in the interior"). Persons and merchandise encountered by CBP at the international border are not only subject to inspection under U.S. law, they also have been or will be abroad and generally subject to the legal authorities of at least one other sovereign. *See Boumelhem*, 339 F.3d at 423.

In addition to longstanding federal court precedent recognizing the constitutional authority of the U.S. government to conduct border searches, numerous federal statutes and regulations also authorize CBP to inspect and examine all individuals and merchandise entering or departing the United States, including all types of personal property, such as electronic devices. *See, e.g.*, 8 U.S.C. §§ 1225, 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a; *see also* 19 C.F.R. § 162.6 ("All persons, baggage, and merchandise arriving in the Customs territory of

the United States from places outside thereof are liable to inspection and search by a Customs officer."). These authorities support CBP's enforcement and administration of federal law at the border and facilitate the inspection of merchandise and people to fulfill the immigration, customs, agriculture, and counterterrorism missions of the Department. This includes, among other things, the responsibility to "ensure the interdiction of persons and goods illegally entering or exiting 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"; "safeguard the borders of the United States to protect against the entry of dangerous goods"; "enforce and administer all immigration laws"; "deter and prevent the illegal entry of terrorists, terrorist weapons, persons, and contraband"; and "conduct inspections at [] ports of entry to safeguard the United States from terrorism and illegal entry of persons." 6 U.S.C. § 211.

CBP must conduct border searches of electronic devices in accordance with statutory and regulatory authorities and applicable judicial precedent. CBP's broad authority to conduct border searches is well-established, and courts have rejected a categorical exception to the border search doctrine for electronic devices. Nevertheless, as a policy matter, this Directive imposes certain requirements, above and beyond prevailing constitutional and legal requirements, to ensure that the authority for border search of electronic devices is exercised judiciously, responsibly, and consistent with the public trust.

5 PROCEDURES

5.1 Border Searches

5.1.1 Border searches may be performed by an Officer or other individual authorized to perform or assist in such searches (e.g., under 19 U.S.C. § 507).

5.1.2 Border searches of electronic devices may include searches of the information stored on the device when it is presented for inspection or during its detention by CBP for an inbound or outbound border inspection. The border search will include an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode), or, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity. Officers should also take care to ensure, throughout the course of a border search, that they do not take actions that would make any changes to the contents of the device.

5.1.3 Basic Search. Any border search of an electronic device that is not an advanced search, as described below, may be referred to as a basic search. In the course of a basic search, with or without suspicion, an Officer may examine an electronic device and may review and analyze information encountered at the border, subject to the requirements and limitations provided herein and applicable law.

5.1.4 Advanced Search. An advanced search is 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. In instances in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval at the Grade 14 level or higher (or a manager with comparable responsibilities), an Officer may perform an advanced search of an electronic device. Many factors may create reasonable suspicion or constitute a national security concern; examples include the existence of a relevant national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list.

5.1.5 Searches of electronic devices will be documented in appropriate CBP systems, and advanced searches should be conducted in the presence of a supervisor. In circumstances where operational considerations prevent a supervisor from remaining present for the entire advanced search, or where supervisory presence is not practicable, the examining Officer shall, as soon as possible, notify the appropriate supervisor about the search and any results thereof.

5.1.6 Searches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, officer safety, or other operational considerations that make it inappropriate to permit the individual to remain present. Permitting an individual to remain present during a search does not necessarily mean that the individual shall observe the search itself. If permitting an individual to observe the search could reveal law enforcement techniques or potentially compromise other operational considerations, the individual will not be permitted to observe the search itself.

5.2 Review and Handling of Privileged or Other Sensitive Material

5.2.1 Officers encountering information they identify as, or that is asserted to be, protected by the attorney-client privilege or attorney work product doctrine shall adhere to the following procedures.

5.2.1.1 The Officer shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information.

5.2.1.2 Prior to any border search of files or other materials over which a privilege has been asserted, the Officer will contact the CBP Associate/Assistant Chief Counsel office. In coordination with the CBP Associate/Assistant Chief Counsel office, which will coordinate with the U.S. Attorney's Office as needed, Officers will ensure the segregation of any privileged material from other information examined during a border search to ensure that any privileged material is handled appropriately while also ensuring that CBP accomplishes its critical border security mission. This segregation process will occur through the establishment and employment of a Filter Team composed of legal and operational representatives, or through another appropriate measure with written concurrence of the CBP Associate/Assistant Chief Counsel office.

5.2.1.3 At the completion of the CBP review, unless any materials are identified that indicate an imminent threat to homeland security, copies of materials maintained by CBP and determined to be privileged will be destroyed, except for any copy maintained in coordination with the CBP Associate/Assistant Chief Counsel office solely for purposes of complying with a litigation hold or other requirement of law.

5.2.2 Other possibly sensitive information, such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy. Questions regarding the review of these materials shall be directed to the CBP Associate/Assistant Chief Counsel office, and this consultation shall be noted in appropriate CBP systems.

5.2.3 Officers encountering business or commercial information in electronic devices shall treat such information as business confidential information and shall protect that information from unauthorized disclosure. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws, as well as CBP policies, may govern or restrict the handling of the information. Any questions regarding the handling of business or commercial information may be directed to the CBP Associate/Assistant Chief Counsel office or the CBP Privacy Officer, as appropriate.

5.2.4 Information that is determined to be protected by law as privileged or sensitive will only be shared with agencies or entities that have mechanisms in place to protect appropriately such information, and such information will only be shared in accordance with this Directive.

5.3 Review and Handling of Passcode-Protected or Encrypted Information

5.3.1 Travelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents. If presented with an electronic device containing information that is protected by a passcode or encryption or other security mechanism, an Officer may request the individual's assistance in presenting the electronic device and the information contained therein in a condition that allows inspection of the device and its contents. Passcodes or other means of access may be requested and retained as needed to facilitate the examination of an electronic device or information contained on an electronic device, including information on the device that is accessible through software applications present on the device that is being inspected or has been detained, seized, or retained in accordance with this Directive.

5.3.2 Passcodes and other means of access obtained during the course of a border inspection will only be utilized to facilitate the inspection of devices and information subject to border search, will be deleted or destroyed when no longer needed to facilitate the search of a given device, and may not be utilized to access information that is only stored remotely.

5.3.3 If an Officer is unable to complete an inspection of an electronic device because it is protected by a passcode or encryption, the Officer may, in accordance with section 5.4 below, detain the device pending a determination as to its admissibility, exclusion, or other disposition.

5.3.4 Nothing in this Directive limits CBP's ability, with respect to any device presented in a manner that is not readily accessible for inspection, to seek technical assistance, or to use external equipment or take other reasonable measures, or in consultation with the CBP Associate/Assistant Chief Counsel office to pursue available legal remedies, to render a device in a condition that allows for inspection of the device and its contents.

5.4 Detention and Review in Continuation of Border Search of Information

5.4.1 Detention and Review by CBP

An Officer may detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days. Devices must be presented in a manner that allows CBP to inspect their contents. Any device not presented in such a manner may be subject to exclusion, detention, seizure, or other appropriate action or disposition.

5.4.1.1 Approval of and Time Frames for Detention. Supervisory approval is required for detaining electronic devices, or copies of information contained therein, for continuation of a border search after an individual's departure from the port or other location of detention. Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent level manager approval is required to extend any such detention beyond five (5) days. Extensions of detentions exceeding fifteen (15) days must be approved by the Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent manager, and may be approved and re-approved in increments of no more than seven (7) days. Approvals for detention and any extension thereof shall be noted in appropriate CBP systems.

5.4.1.2 Destruction. Except as noted in section 5.5 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.4, there is no probable cause to seize the device or the information contained therein, any copies of the information held by CBP must be destroyed, and any electronic device must be returned. Upon this determination, the copy of the information will be destroyed as expeditiously as possible, but no later than seven (7) days after such determination unless circumstances require additional time, which must be approved by a supervisor and documented in an appropriate CBP system and which must be no later than twenty-one (21) days after such determination. The destruction shall be noted in appropriate CBP systems.

5.4.1.3 Notification of Border Search. When a border search of information is conducted on an electronic device, the individual subject to search will be notified of the purpose and authority for such search, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search. If the Officer or other appropriate CBP official determines that the fact of conducting this search cannot be disclosed to the individual transporting the device without

impairing national security, law enforcement, officer safety, or other operational interests, notification may be withheld.

5.4.1.4 Custody Receipt. If CBP determines it is necessary to detain temporarily an electronic device to continue the search, the Officer detaining the device shall issue a completed Form 6051D to the individual prior to the individual's departure.

5.4.2 Assistance

Officers may request assistance that may be needed to access and search an electronic device and the information stored therein. Except with respect to assistance sought within CBP or from ICE, the following subsections of 5.4.2 govern requests for assistance.

5.4.2.1 Technical Assistance. Officers may sometimes need technical assistance to render a device and its contents in a condition that allows for inspection. For example, Officers may encounter a device or information that is not readily accessible for inspection due to encryption or password protection. Officers may also require translation assistance to inspect information that is in a foreign language. In such situations, Officers may convey electronic devices or copies of information contained therein to seek technical assistance.

5.4.2.2 Subject Matter Assistance – With Reasonable Suspicion or National Security Concern. Officers may encounter information that requires referral to subject matter experts to determine the meaning, context, or value of information contained therein as it relates to the laws enforced or administered by CBP. Therefore, Officers may convey electronic devices or copies of information contained therein for the purpose of obtaining subject matter assistance when there is a national security concern or they have reasonable suspicion of activities in violation of the laws enforced or administered by CBP.

5.4.2.3 Approvals for Seeking Assistance. Requests for assistance require supervisory approval and shall be properly documented and recorded in CBP systems. If an electronic device is to be detained after the individual's departure, the Officer detaining the device shall execute a Form 6051D and provide a copy to the individual prior to the individual's departure. All transfers of the custody of the electronic device will be recorded on the Form 6051D.

5.4.2.4 Electronic devices should be transferred only when necessary to render the requested assistance. Otherwise, a copy of data from the device should be conveyed in lieu of the device in accordance with this Directive.

5.4.2.5 When an electronic device or information contained therein is conveyed for assistance, the individual subject to search will be notified of the conveyance unless the Officer or other appropriate CBP official determines, in consultation with the receiving agency or other entity as appropriate, that notification would impair national security, law enforcement, officer safety, or other operational interests. If CBP seeks assistance for counterterrorism purposes, if a relevant national security-related lookout applies, or if the individual is on a government-operated and government-vetted terrorist watch list, the individual will not be notified of the conveyance, the existence of a relevant national security-related lookout, or his or her presence on a watch list.

When notification is made to the individual, the Officer will annotate the notification in CBP systems and on the Form 6051D.

5.4.3 Responses and Time for Assistance

5.4.3.1 Responses Required. Agencies or entities receiving a request for assistance in conducting a border search are expected to provide such assistance as expeditiously as possible. Where subject matter assistance is requested, responses should include all appropriate findings, observations, and conclusions relating to the laws enforced or administered by CBP.

5.4.3.2 Time for Assistance. Responses from assisting agencies or entities are expected in an expeditious manner so that CBP may complete the border search in a reasonable period of time. Unless otherwise approved by the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager, responses should be received within fifteen (15) days. If the assisting agency or entity is unable to respond in that period of time, the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager may permit extensions in increments of seven (7) days.

5.4.3.3 Revocation of a Request for Assistance. If at any time a CBP supervisor involved in a request for assistance is not satisfied with the assistance provided, the timeliness of assistance, or any other articulable reason, the request for assistance may be revoked, and the CBP supervisor may require the assisting agency or entity to return to CBP all electronic devices provided, and any copies thereof, as expeditiously as possible, except as noted in 5.5.2.3. Any such revocation shall be documented in appropriate CBP systems. When CBP has revoked a request for assistance because of the lack of a timely response, CBP may initiate the request with another agency or entity pursuant to the procedures outlined in this Directive.

5.4.3.4 Destruction. Except as noted in section 5.5.1 below or elsewhere in this Directive, if after reviewing information, probable cause to seize the device or the information from the device does not exist, CBP will retain no copies of the information.

5.5 Retention and Sharing of Information Found in Border Searches

5.5.1 Retention and Sharing of Information Found in Border Searches

5.5.1.1 Retention with Probable Cause. Officers may seize and retain an electronic device, or copies of information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is probable cause to believe that the device, or copy of the contents from the device, contains evidence of a violation of law that CBP is authorized to enforce or administer.

5.5.1.2 Retention of Information in CBP Privacy Act-Compliant Systems. Without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the applicable system of records notice. For example, information

collected in the course of immigration processing for the purposes of present and future admissibility of an alien may be retained in the A-file, Central Index System, TECS, and/or E3 or other systems as may be appropriate and consistent with the policies governing such systems.

5.5.1.3 Sharing Generally. Nothing in this Directive limits the authority of CBP to share copies of information contained in electronic devices (or portions thereof), which are retained in accordance with this Directive, with federal, state, local, and foreign law enforcement agencies to the extent consistent with applicable law and policy.

5.5.1.4 Sharing of Terrorism Information. Nothing in this Directive is intended to limit the sharing of terrorism-related information to the extent the sharing of such information is authorized by statute, Presidential Directive, or DHS policy. Consistent with 6 U.S.C. § 122(d)(2) and other applicable law and policy, CBP, as a component of DHS, will promptly share any terrorism information encountered in the course of a border search with entities of the federal government responsible for analyzing terrorist threat information. In the case of such terrorism information sharing, the entity receiving the information will be responsible for providing CBP with all appropriate findings, observations, and conclusions relating to the laws enforced by CBP. The receiving entity will be responsible for managing retention and disposition of information it receives in accordance with its own legal authorities and responsibilities.

5.5.1.5 Safeguarding Data During Storage and Conveyance. CBP will appropriately safeguard information retained, copied, or seized under this Directive and during conveyance. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking copies to ensure appropriate disposition, and other safeguards during conveyance such as password protection or physical protections. Any suspected loss or compromise of information that contains personal data retained, copied, or seized under this Directive must be immediately reported to the CBP Office of Professional Responsibility and to the Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager.

5.5.1.6 Destruction. Except as noted in this section or elsewhere in this Directive, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information.

5.5.2 Retention by Agencies or Entities Providing Technical or Subject Matter Assistance

5.5.2.1 During Assistance. All electronic devices, or copies of information contained therein, provided to an assisting agency or entity may be retained for the period of time needed to provide the requested assistance to CBP or in accordance with section 5.5.2.3 below.

5.5.2.2 Return or Destruction. CBP will request that at the conclusion of the requested assistance, all information be returned to CBP as expeditiously as possible, and that the assisting agency or entity advise CBP in accordance with section 5.4.3 above. In addition, the assisting agency or entity should destroy all copies of the information conveyed unless section 5.5.2.3 below applies. In the event that any electronic devices are conveyed, they must not be destroyed;

they are to be returned to CBP unless seized by an assisting agency based on probable cause or retained per 5.5.2.3.

5.5.2.3 Retention with Independent Authority. If an assisting federal agency elects to continue to retain or seize an electronic device or information contained therein, that agency assumes responsibility for processing the retention or seizure. Copies may be retained by an assisting federal agency only if and to the extent that it has the independent legal authority to do so – for example, when the information relates to terrorism or national security and the assisting agency is authorized by law to receive and analyze such information. In such cases, the retaining agency should advise CBP of its decision to retain information under its own authority.

5.6 Reporting Requirements

5.6.1 The Officer performing the border search of information shall be responsible for completing all after-action reporting requirements. This responsibility includes ensuring the completion of all applicable documentation such as the Form 6051D when appropriate, and creation and/or updating records in CBP systems. Reports are to be created and updated in an accurate, thorough, and timely manner. Reports must include all information related to the search through the final disposition including supervisory approvals and extensions when appropriate.

5.6.2 In instances where an electronic device or copy of information contained therein is forwarded within CBP as noted in section 5.4.1, the receiving Officer is responsible for recording all information related to the search from the point of receipt forward through the final disposition.

5.6.3 Reporting requirements for this Directive are in addition to, and do not replace, any other applicable reporting requirements.

5.7 Management Requirements

5.7.1 The duty supervisor shall ensure that the Officer completes a thorough inspection and that all notification, documentation, and reporting requirements are accomplished.

5.7.2 The appropriate CBP second-line supervisor shall approve and monitor the status of the detention of all electronic devices or copies of information contained therein.

5.7.3 The appropriate CBP second-line supervisor shall approve and monitor the status of the transfer of any electronic device or copies of information contained therein for translation, decryption, or subject matter assistance from another agency or entity.

5.7.4 The Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager shall establish protocols to monitor the proper documentation and recording of searches conducted pursuant to this Directive and the detention, transfer, and final disposition of electronic devices or copies of

information contained therein in order to ensure compliance with the procedures outlined in this Directive.

5.7.5 Officers will ensure, in coordination with field management as appropriate, that upon receipt of any subpoena or other request for testimony or information regarding the border search of an electronic device in any litigation or proceeding, notification is made to the appropriate CBP Associate/Assistant Chief Counsel office.

6 MEASUREMENT. CBP Headquarters will continue to develop and maintain appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from CBP systems using data elements entered by Officers pursuant to this Directive.

7 AUDIT. CBP Management Inspection will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

8 NO PRIVATE RIGHT CREATED. This Directive is an internal policy statement of U.S. Customs and Border Protection and does not create or confer any rights, privileges, or benefits on any person or party.

9 REVIEW. This Directive shall be reviewed and updated, as necessary, at least every three years.

10 DISCLOSURE. This Directive may be shared with the public.

11 SUPERSEDES. Procedures for Border Search/Examination of Documents, Paper, and Electronic Information (July 5, 2007) and Policy Regarding Border Search of Information (July 16, 2008), to the extent they pertain to electronic devices; CBP Directive No. 3340-049, Border Searches of Electronic Devices Containing Information (August 20, 2009).

Acting Commissioner

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
ICE Policy System

DISTRIBUTION:	**ICE**
DIRECTIVE NO.:	**7-6.1**
ISSUE DATE:	**August 18, 2009**
EFFECTIVE DATE:	**August 18, 2009**
REVIEW DATE:	**August 18, 2012**
SUPERSEDES:	**See Section 3 Below.**

DIRECTIVE TITLE: BORDER SEARCHES OF ELECTRONIC DEVICES

1. PURPOSE and SCOPE.

1.1. This Directive provides legal guidance and establishes policy and procedures within U.S. Immigration and Customs Enforcement (ICE) with regard to border search authority to search, detain, seize, retain, and share information contained in electronic devices possessed by individuals at the border, the functional equivalent of the border, and the extended border to ensure compliance with customs, immigration, and other laws enforced by ICE. This Directive applies to searches of electronic devices of all persons arriving in, departing from, or transiting through the United States, unless specified otherwise.

1.2. This Directive applies to border search authority only. Nothing in this Directive limits the authority of ICE Special Agents to act pursuant to other authorities such as a warrant, a search incident to arrest, or a routine inspection of an applicant for admission.

2. AUTHORITIES/REFERENCES. 8 U.S.C. § 1357 and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. § 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. § 401 and other laws relating to exports; and the December 12, 2008, ICE Office of Investigations (OI) guidance entitled "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices."

3. SUPERSEDED/CANCELLED POLICY/SUMMARY OF CHANGES. ICE Directive No. 7-6.0 entitled "Border Searches of Documents and Electronic Media" is hereby superseded as it relates to electronic devices. Additionally, all other issuances on this subject issued by ICE prior to the date of this Directive are hereby superseded as they relate to searches of electronic devices, with the exception of the March 5, 2007, OI guidance entitled "Field Guidance on Handling Detained or Seized Electronic Media from Persons of National Security Interest at Ports of Entry" and the December 12, 2008, OI guidance entitled "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media."

4. BACKGROUND. ICE is responsible for ensuring compliance with customs, immigration, and other Federal laws at the border. To that end, Special Agents may review and analyze computers, disks, hard drives, and other electronic or digital storage devices. These searches are part of ICE's long-standing practice and are essential to enforcing the law at the United States border. Searches of electronic devices are a crucial tool for detecting information concerning terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography; laundering monetary instruments; violations of copyright or trademark laws; and evidence of embargo violations or other import or export control laws.

5. DEFINITIONS. The following definitions are provided for the purposes of this Directive:

5.1. Assistance. The use of third party analytic resources such as language processing, decryption, and subject matter expertise, to assist ICE in viewing the information contained in electronic devices or in determining the meaning, context, or value of information contained therein.

5.2. Electronic Devices. Any item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices.

6. POLICY.

6.1. ICE Special Agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion, consistent with the guidelines and applicable laws set forth herein. Assistance to complete a border search may be sought from other Federal agencies and non-Federal entities, on a case by case basis, as appropriate.

6.2. When U.S. Customs and Border Protection (CBP) detains, seizes, or retains electronic devices, or copies of information therefrom, and turns such over to ICE for analysis and investigation (with appropriate documentation), ICE policy will apply once it is received by ICE.

6.3. Nothing in this policy limits the authority of Special Agents to make written notes or reports or to document impressions relating to a border encounter in ICE's paper or electronic recordkeeping systems.

7. RESPONSIBILITIES.

7.1. The Directors of OI, the Office of Professional Responsibility (OPR), and the Office of International Affairs (OIA) have oversight over the implementation of the provisions of this Directive.

7.2. Special Agents in Charge (SACs) and Attachés are responsible for:

1) Implementing the provisions of this Directive and ensuring that Special Agents in their area of responsibility (AOR) receive a copy of this Directive and are familiar with its contents;

2) Ensuring that Special Agents in their AOR have completed any training programs relevant to border searches of electronic devices, including constitutional, privacy, civil rights, and civil liberties training related to such searches, as may be required by ICE Headquarters; and

3) Maintaining appropriate mechanisms for internal audit and review of compliance with the procedures outlined in this Directive. (See "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices" memo dated December 12, 2008.)

7.3. Attachés are responsible for ensuring coordination with their host countries, as appropriate, before conducting any such border search outside of the United States.

7.4. When ICE receives electronic devices, or copies of information therefrom, from CBP for analysis and investigation, ICE Special Agents are responsible for advising CBP of the status of any such analysis within 10 calendar days, and periodically thereafter, so that CBP records may be updated as appropriate. For example, "search ongoing"; "completed with negative results"; "returned to traveler"; or "seized as evidence of a crime."

7.5. Special Agents are responsible for complying with the provisions of this Directive, knowing the limits of ICE authority, using this authority judiciously, and ensuring comprehension and completion of any training programs relevant to border searches of electronic devices as may be required by ICE.

8. PROCEDURES.

8.1. Border Searches by ICE Special Agents.

1) Authorization to Conduct Border Search. Border searches of electronic devices must be performed by an ICE Special Agent who meets the definition of "customs officer" under 19 U.S.C. § 1401(i), or another properly authorized officer with border search authority, such as a CBP Officer or Border Patrol Agent, persons cross designated by ICE as customs officers, and persons whose assistance to ICE is demanded under 19 U.S.C. § 507.

2) Knowledge and Presence of the Traveler. To the extent practicable, border searches should be conducted in the presence of, or with the knowledge of, the traveler. When not practicable due to law enforcement, national security, or other operational concerns, such circumstances are to be noted by the Special Agent in appropriate ICE systems. Permitting an individual to be present in the room during a search does not necessarily mean that the individual will be permitted to witness the search itself. If permitting an individual to witness the search itself could reveal law enforcement

techniques or potentially compromise other operational concerns, the individual will not be permitted to observe the search.

3) Consent Not Needed. At no point during a border search of electronic devices is it necessary to ask the traveler for consent to search.

4) Continuation of the Border Search. At any point during a border search, electronic devices, or copies of information therefrom, may be detained for further review either on-site at the place of detention or at an off-site location, including a location associated with a demand for assistance from an outside agency or entity (see Section 8.4).

5) Originals. In the event electronic devices are detained, the Special Agent should consider whether it is appropriate to copy the information therefrom and return the device. When appropriate, given the facts and circumstances of the matter, any such device should be returned to the traveler as soon as practicable. Consultation with the Office of the Chief Counsel is recommended when determining whether to retain a device in an administrative immigration proceeding. Devices will be returned to the traveler as expeditiously as possible at the conclusion of a negative border search.

8.2. Chain of Custody.

1) Detentions of electronic devices. Whenever ICE detains electronic devices, or copies of information therefrom, the Special Agent will initiate the correct chain of custody form or other appropriate documentation.

2) Seizures of electronic devices for criminal purposes. Whenever ICE seizes electronic devices, or copies of information therefrom, the Special Agent is to enter the seizure into the appropriate ICE systems. Additionally, the seizing agent must complete the correct chain of custody form or other appropriate documentation.

3) Retention of electronic devices for administrative immigration purposes. Whenever ICE retains electronic devices, or copies of information therefrom, or portions thereof, for administrative immigration purposes pursuant to 8 U.S.C. § 1357, the Special Agent is to record such retention in appropriate ICE systems and is to include the location of the retained files, a summary thereof, and the purpose for retention.

4) Notice to traveler. Whenever ICE detains, seizes, or retains original electronic devices, the Special Agent is to provide the traveler with a copy of the applicable chain of custody form or other appropriate documentation.

8.3. Duration of Border Search.

1) Special Agents are to complete the search of detained electronic devices, or copies of information therefrom, in a reasonable time given the facts and circumstances of the particular search. Searches are generally to be completed within 30 calendar days of

the date of detention, unless circumstances exist that warrant more time. Such circumstances must be documented in the appropriate ICE systems. Any detention exceeding 30 calendar days must be approved by a Group Supervisor or equivalent, and approved again every 15 calendar days thereafter, and the specific justification for additional time documented in the appropriate ICE systems.

2) Special Agents seeking assistance from other Federal agencies or non-Federal entities are responsible for ensuring that the results of the assistance are received in a reasonable time (see Section 8.4(5)).

3) In determining "reasonable time," courts have reviewed the elapsed time between the detention and the completion of the border search, taking into account any additional facts and circumstances unique to the case. As such, ICE Special Agents are to document the progress of their searches, for devices and copies of information therefrom, and should consider the following factors:

   a) The amount of information needing review;

   b) Whether the traveler was deprived of his or her property and, if so, whether the traveler was given the option of continuing his or her journey with the understanding that ICE would return the property once its border search was complete or a copy could be made;

   c) Whether assistance was sought and the type of such assistance;

   d) Whether and when ICE followed up with the agency or entity providing assistance to ensure a timely review;

   e) Whether the traveler has taken affirmative steps to prevent the search of his or her property in a timely fashion; and

   f) Any unanticipated exigency that may arise.

8.4. Assistance by Other Federal Agencies and Non-Federal Entities.

1) Translation, Decryption, and Other Technical Assistance.

   a) During a border search, Special Agents may encounter information in electronic devices that presents technical difficulties, is in a foreign language, and/or encrypted. To assist ICE in conducting a border search or in determining the meaning of such information, Special Agents may demand translation, decryption, and/or technical assistance from other Federal agencies or non-Federal entities.

   b) Special Agents may demand such assistance absent individualized suspicion.

   c) Special Agents shall document such demands in appropriate ICE systems.

2) Subject Matter Assistance.

   a) During a border search, Special Agents may encounter information in electronic devices that are not in a foreign language or encrypted, or that do not require other technical assistance, in accordance with Section 8.4(1), but that nevertheless requires referral to subject matter experts to determine whether the information is relevant to the laws enforced and administered by ICE. For the purpose of obtaining such subject matter expertise, Special Agents may create and transmit a copy of such information to other Federal agencies or non-Federal entities.

   b) Special Agents may demand such assistance when they have reasonable suspicion of activities in violation of the laws enforced by ICE.

   c) Special Agents shall document such demands in appropriate ICE systems.

3) Demand Letter. Unless otherwise governed by a Memorandum of Understanding or similar mechanism, each demand for assistance is to be in writing (e.g., letter or email), approved by a supervisor, and documented in the appropriate ICE systems. Demands are to detail the context of the search requested, ICE's legal parameters regarding the search, retention, and sharing of any information found during the assistance, and relevant timeframes, including those described in this Directive.

4) Originals. For the purpose of obtaining subject matter assistance, Special Agents may create and transmit copies of information to other Federal agencies or non-Federal entities. Original electronic devices should be transmitted only when necessary to render the demanded assistance.

5) Time for Assistance and Responses Required.

   a) Assistance is to be accomplished within a reasonable period of time in order to preserve the status of the electronic devices and the integrity of the border search.

   b) It is the responsibility of the Special Agent demanding the assistance to ensure timely responses from assisting agencies or entities and to act in accord with section 8.3 of this Directive. In addition, Special Agents shall:

      i) Inform assisting agencies or entities that they are to provide results of assistance as expeditiously as possible;

      ii) Ensure that assisting agencies and entities are aware that responses to ICE must include any findings, observations, and conclusions drawn from their review that may relate to the laws enforced by ICE;

iii) Contact the assisting agency or entity to get a status report on the demand within the first 30 calendar days;

iv) Remain in communication with the assisting agency or entity until results are received;

v) Document all communications and actions in appropriate ICE systems; and

vi) Consult with a supervisor to determine appropriate action if the timeliness of results is a concern. If a demand for assistance is revoked, the Special Agent is to ensure all electronic devices are returned to ICE as expeditiously as possible.

8.5. Retention, Sharing, Safeguarding, And Destruction.

1) By ICE

a) Seizure and Retention with Probable Cause. When Special Agents determine there is probable cause of unlawful activity—based on a review of information in electronic devices or on other facts and circumstances—they may seize and retain the electronic device or copies of information therefrom, or relevant portions thereof, as authorized by law.

b) Retention of Information in ICE Systems. To the extent authorized by law, ICE may retain information relevant to immigration, customs, and other law enforcement matters in ICE systems if such retention is consistent with the privacy and data protection policies of the system in which such information is retained. For example, information entered into TECS during the course of an investigation will be retained consistent with the policies governing TECS.

c) Sharing. Copies of information from electronic devices, or portions thereof, which are retained in accordance with this section, may be shared by ICE with Federal, state, local, and foreign law enforcement agencies in accordance with applicable law and policy. Sharing must be in compliance with the Privacy Act and applicable ICE privacy policies, such as the ICE Search, Arrest, and Seizure System of Records Notice.

d) Safeguarding Data During Storage and Transmission. ICE will appropriately safeguard information detained, copied, retained, or seized under this directive while in ICE custody and during transmission to an outside entity. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking originals and copies to ensure appropriate disposition, and appropriate safeguards during transmission such as encryption of electronic data or physical protections (e.g., locked containers). Any suspected loss or compromise of information that contains personal data detained, copied, or seized under this directive must be reported immediately to the ICE Service Desk.

e) Destruction. Copies of information from electronic devices, or portions thereof, determined to be of no relevance to ICE will be destroyed in accordance with ICE policy governing the particular form of information. Such destruction must be accomplished by the responsible Special Agent within seven business days after conclusion of the border search unless circumstances require additional time, which must be approved by a supervisor and documented in appropriate ICE systems. All destructions must be accomplished no later than 21 calendar days after conclusion of the border search.

2) By Assisting Agencies

a) Retention during Assistance. All electronic devices, whether originals or copies of information therefrom, provided to an assisting Federal agency may be retained by that agency for the period of time needed to provide the requested assistance to ICE.

b) Return or Destruction. At the conclusion of the requested assistance, all electronic devices and data must be returned to ICE as expeditiously as possible. In the alternative, the assisting Federal agency may certify to ICE that any copies in its possession have been destroyed or it may advise ICE in accordance with Section 8.5(2)(c). In the event that any original electronic devices were transmitted, they must not be destroyed; they are to be returned to ICE.

c) Retention with Independent Authority. Copies may be retained by an assisting Federal agency only if and to the extent that it has the independent legal authority to do so – for example, when the information is of national security or intelligence value. In such cases, the retaining agency must advise ICE of its decision to retain certain information on its own authority. In the event that any original electronic devices were transmitted, the assisting Federal agency may make a copy of information therefrom for its retention; however, any originals must be returned to ICE.

3) By Non-Federal Entities

a) ICE may provide copies of information from electronic devices to an assisting non-Federal entity, such as a private language translation or data decryption service, only for the period of time needed by that entity to render the requested assistance.

b) Upon the completion of assistance, all copies of the information in the possession of the entity must be returned to ICE as expeditiously as possible. Any latent copies of the electronic data on the systems of the non-Federal entity must also be destroyed so that recovery of the data is impractical.

8.6. Review, Handling, and Sharing of Certain Types of Information.

1) Border Search. All electronic devices crossing U.S. borders are subject to border search; a claim of privilege or personal information does not prevent the search of a traveler's information at the border. However, the nature of certain types of information are subject to special handling by Special Agents, whether through policy or laws such as the Privacy Act and the Trade Secrets Act.

2) Types of Information

a) Business or Commercial Information. If, in the course of a border search, Special Agents encounter business or commercial information, such information is to be treated as business confidential information. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws may specifically govern or restrict handling of the information, including criminal penalties for unauthorized disclosure.

b) Legal Information. Special Agents may encounter information that appears to be legal in nature, or an individual may assert that certain information is protected by the attorney-client or attorney work product privilege. If Special Agents suspect that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of ICE, the ICE Office of the Chief Counsel or the appropriate U.S. Attorney's Office must be contacted before beginning or continuing a search of the document and this consultation shall be noted in appropriate ICE systems.

c) Other Sensitive Information. Other possibly sensitive information, such as medical records and work-related information carried by journalists shall be handled in accordance with all applicable federal law and ICE policy. Although there is no Federal legal privilege pertaining to the doctor-patient relationship, the inherent nature of medical information warrants special care for such records. Questions regarding the review of these materials shall be directed to the ICE Office of the Chief Counsel and this consultation shall be noted in appropriate ICE systems.

3) Sharing. Information that is determined to be protected by law as privileged or sensitive is to be handled consistent with the laws and policies governing such information.

8.7 Measurement. ICE Headquarters will develop appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from ICE systems using data elements entered by Special Agents pursuant to this Directive.

8.8 **Audit**. ICE Headquarters will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

9. **ATTACHMENTS.** None.

10. **NO PRIVATE RIGHT STATEMENT.** This Directive is an internal policy statement of ICE. It is not intended to, and does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, or other entities, its officers or employees; or any other person.

Approved _____

John Morton
Assistant Secretary
U.S. Immigration and Customs Enforcement

From: [redacted]
Sent: Friday, May 11, 2018 5:19 PM
To: [redacted]
[redacted]
Subject: (0476-18) Broadcast- Legal Update- Border Search of Electronic Devices

HSI HOMELAND SECURITY INVESTIGATIONS
Message from the AD of Domestic Operations

Legal Update Border Search of Electronic Devices

On May 9, 2018, in *United States v. Kolsuz*, the U.S. Court of Appeals for the Fourth Circuit held that the "forensic" examination of a cell phone is a nonroutine border search, requiring some measure of individualized suspicion. --- F.3d ---, 2018 WL 2122085 (4th Cir. 2018). The court, however, determined that it need not resolve whether the proper standard should be reasonable suspicion or probable cause and a warrant.

Although the Office of the Principal Legal Advisor (OPLA) advises Homeland Security Investigations (HSI) nationwide that it should have reasonable suspicion before performing an advanced search of an electronic device (any border search of an electronic device in which external equipment, through a wired or wireless connection, is connected to an electronic device not merely to gain access to the device or its contents but to review, copy, and/or analyze its contents), **this decision creates binding precedent in the jurisdiction of the U.S. Court of Appeals for the Fourth Circuit that at least some level of individualized suspicion is required for such searches;** the only other circuit to have required this standard is the Ninth Circuit Court of Appeals. *See U.S. v. Cotterman*, 709 F.3d 952 (9th Cir. 2013 (en banc).

Formal policy guidance with regard to border searches of electronic devices is forthcoming. In the interim, in order to limit litigation risk, HSI Special Agents and others authorized by HSI to perform border searches, even outside of the Fourth and Ninth Circuits, should no longer perform advanced border searches of electronic

devices without reasonable suspicion. All factors supporting such a standard should be documented in reports of investigation.

If you have any questions on this matter, please contact OPLA imbed counsel.

Limitation on the Applicability of this Guidance. This message is intended to provide internal guidance to the operational components of U.S. Immigration and Customs Enforcement. It does not, is not intended to, shall not be construed to, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any person in any matter, civil or criminal.

[redacted]

Thanks,

Tatum King
Assistant Director, Domestic Operations
Homeland Security Investigations

HSI Domestic Operations / MW
500 12th Street SW, 6th Floor
Washington, D.C. 20536
Email – [redacted]