

No. _____

IN THE
Supreme Court of the United States

ZAINAB MERCHANT; SUHAIB ALLABABIDI; SIDD BIKKANAVAR;
AARON GACH; ISMAIL ABDEL-RASOUL aka ISMA'IL KUSHKUSH;
DIANE MAYE ZORRI; MOHAMMED AKRAM SHIBLY; MATTHEW WRIGHT,

—v.— *Petitioners,*

ALEJANDRO MAYORKAS, SECRETARY OF THE U.S. DEPARTMENT OF
HOMELAND SECURITY, in his official capacity; TROY A. MILLER,
SENIOR OFFICIAL PERFORMING THE DUTIES OF THE COMMISSIONER
OF U.S. CUSTOMS AND BORDER PROTECTION, in his official capacity;
TAE D. JOHNSON, ACTING DIRECTOR OF U.S. IMMIGRATION AND
CUSTOMS ENFORCEMENT, in his official capacity,

Respondents.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES
COURT OF APPEALS FOR THE FIRST CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

Adam Schwartz
Sophia Cope
Saira Hussain
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Jessie J. Rossman
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF
MASSACHUSETTS, INC.
211 Congress Street
Boston, MA 02110

Esha Bhandari
Counsel of Record
Hugh Handeyside
Nathan Freed Wessler
Ben Wizner
Hina Shamsi
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500
ebhandari@aclu.org

David D. Cole
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
915 15th Street, N.W.
Washington, D.C. 20005

QUESTION PRESENTED

Does the Fourth Amendment require that searches of electronic devices at the U.S. border be conducted pursuant to a warrant based on probable cause, or at least pursuant to an officer's determination of reasonable suspicion that the device contains digital contraband?

PARTIES TO THE PROCEEDING

In addition to the parties appearing in the caption of the case on the cover page, Ghassan Alasaad, Nadia Alasaad, and Jérémie Dupin were plaintiffs in the proceedings below.

RELATED PROCEEDINGS

Alasaad v. Mayorkas, U.S. Court of Appeals for the First Circuit, Nos. 20-1077, 20-1081. Corrected Opinion issued February 9, 2021;

Alasaad v. Nielsen, U.S. District Court for the District of Massachusetts, No. 1:17-cv-11730-DJC. Memorandum and Order on parties' cross-motions for summary judgment issued November 12, 2019, and Judgment entered November 21, 2019. Judgment following mandate issued by the Court of Appeals entered on April 21, 2021.

Alasaad v. Nielsen, U.S. District Court for the District of Massachusetts, No. 1:17-cv-11730-DJC. Memorandum and Order denying motion to dismiss issued May 9, 2018.

TABLE OF CONTENTS

QUESTION PRESENTED	i
PARTIES TO THE PROCEEDING	ii
TABLE OF AUTHORITIES	vi
PETITION FOR A WRIT OF CERTIORARI.....	1
OPINIONS BELOW	1
STATEMENT OF JURISDICTION.....	1
CONSTITUTIONAL PROVISION INVOLVED.....	1
STATEMENT OF THE CASE.....	2
REASONS FOR GRANTING THE WRIT	11
I. THE FEDERAL COURTS OF APPEALS ARE DIVIDED ON THE FOURTH AMENDMENT'S REQUIREMENTS FOR BORDER SEARCHES OF ELECTRONIC DEVICES	11
A. The Circuits Have Adopted Conflicting Rules on the Permissible Bounds of Border Searches of Electronic Devices	12
1. The First Circuit.....	12
2. The Ninth Circuit	13
3. The Fourth Circuit.....	13
4. The Eleventh Circuit	14
B. The Circuits Are Divided on Whether and What Level of Individualized Suspicion Is Required.....	15

C.	The Circuits Are Divided on the Permissible Scope of Warrantless Border Device Searches.....	16
II.	THIS CASE PRESENTS AN IMPORTANT AND RECURRING QUESTION ON CONSTITUTIONAL PRIVACY RIGHTS IN THE DIGITAL AGE.....	17
III.	THIS CASE IS AN IDEAL VEHICLE TO RESOLVE THESE CONFLICTS.....	20
IV.	THE DECISION BELOW IS INCORRECT ...	23
A.	The First Circuit Erred in Holding that a Warrant Is Not Required for Electronic Device Searches at the Border.....	24
1.	<i>Riley</i> 's Reasoning Compels a Warrant Requirement for Border Searches of Electronic Devices.....	24
2.	This Court Has Left Open the Possibility That Certain Border Searches Require a Warrant.....	30
3.	The First Circuit Misconstrued This Court's Precedent on Warrant Exceptions.....	30
B.	The First Circuit Erred by Not Holding, in the Alternative, that all Device Searches at the Border Require Reasonable Suspicion that the Device Contains Digital Contraband.....	32
	CONCLUSION.....	35

APPENDIX

Appendix A, Court of appeals opinion, Feb. 9, 2021	1a
Appendix B, District court judgment, Nov. 21, 2019.....	29a
Appendix C, District court summary judgment memorandum and order, Nov. 12, 2019.....	32a
Appendix D, District court memorandum and order denying motion to dismiss, May 9, 2018.....	92a
Appendix E, Plaintiffs’ supplemental statement of undisputed material facts, July 12, 2019 ...	156a
Appendix F, Plaintiffs’ response and reply in support of statement of undisputed material facts, July 3, 2019	159a
Appendix G, Homeland Security Investigations legal update, May 11, 2018.....	284a
Appendix H, U.S. Customs and Border Protection policy directive, Jan. 4, 2018	286a
Appendix I, U.S. Immigration and Customs Enforcement policy directive, Aug. 18, 2009	311a
Appendix J, District court final judgment, April 21, 2021.....	332a

TABLE OF AUTHORITIES

CASES

<i>Arizona v. Gant</i> , 556 U.S. 332 (2009)	31
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018)	18, 19
<i>Carroll v. United States</i> , 267 U.S. 132 (1925).	26
<i>City of Indianapolis v. Edmond</i> , 531 U.S. 32 (2000)	27
<i>Collins v. Virginia</i> , 138 S. Ct. 1663 (2018)	32
<i>Florida v. Royer</i> , 460 U.S. 491(1983)	18
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	18
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001)	18
<i>Riley v. California</i> , 573 U.S. 373 (2014)	<i>passim</i>
<i>United States v. Caballero</i> , 178 F. Supp. 3d 1008 (S.D. Cal. 2016)	20
<i>United States v. 12 200-Foot Reels of Super 8mm. Film</i> , 413 U.S. 123 (1973).....	27
<i>United States v. Aigbekaen</i> , 943 F.3d 713 (4th Cir. 2019)	14, 16
<i>United States v. Cano</i> , 934 F.3d 1002 (9th Cir. 2019)	<i>passim</i>

<i>United States v. Cotterman</i> , 709 F.3d 952 (9th Cir. 2013)	6, 12, 13
<i>United States v. Flores-Montano</i> , 541 U.S. 149 (2004)	30
<i>United States v. Jones</i> , 565 U.S. 400 (2012)	18
<i>United States v. Kolsuz</i> , 890 F.3d 133 (4th Cir. 2018)	<i>passim</i>
<i>United States v. Molina-Isidoro</i> , 884 F.3d 287 (5th Cir. 2018)	28
<i>United States v. Molina-Isidoro</i> , 267 F. Supp. 3d 900 (W.D. Tex. 2016)	20
<i>United States v. Montoya de Hernandez</i> , 473 U.S. 531 (1985)	<i>passim</i>
<i>United States v. Thirty-Seven Photographs</i> , 402 U.S. 363 (1971)	27
<i>United States v. Tousef</i> , 890 F.3d 1227 (11th Cir. 2018)	14, 15, 16
<i>United States v. Vergara</i> , 884 F.3d 1309 (11th Cir. 2018)	<i>passim</i>

CONSTITUTION

U.S. Const. amend. IV	<i>passim</i>
-----------------------------	---------------

OTHER AUTHORITIES

<i>CBP Statement on Border Search of Electronic Devices</i> (Oct. 30, 2019), https://perma.cc/JX8K- BN5B	7
Pet. for a Writ of Cert., <i>United States v. Cano</i> , No. 20-1043 (Jan. 29, 2021).....	23

PETITION FOR A WRIT OF CERTIORARI

Petitioners Zainab Merchant, Suhaib Allababidi, Sidd Bikkannavar, Aaron Gach, Ismail Abdel-Rasoul aka Isma'il Kushush, Diane Maye Zorri, Mohammed Akram Shibly, and Matthew Wright respectfully petition for a writ of certiorari to review the judgment of the United States Court of Appeals for the First Circuit.

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. 1a) is reported at *Alasaad v. Mayorikas*, 988 F.3d 8 (1st Cir. 2021). The district court memorandum and order on cross-motions for summary judgment (Pet. App. 32a) is reported at *Alasaad v. Nielsen*, 419 F. Supp. 3d 142 (D. Mass. 2019). The district court judgment entering injunctive and declaratory relief (Pet. App. 29a) is not reported. The district court judgment vacating injunctive and declaratory relief (Pet. App. 332a) is not reported.

STATEMENT OF JURISDICTION

The court of appeals issued its decision on February 9, 2021 (Pet. App. 1a). This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment to the U.S. Constitution provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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.

STATEMENT OF THE CASE

Petitioners filed a civil action against Respondents the U.S. Department of Homeland Security (“DHS”), U.S. Customs and Border Protection (“CBP”), and U.S. Immigration and Customs Enforcement (“ICE”), after being subjected to highly invasive searches of their cell phones, laptops, and other electronic devices at the U.S. border. As the undisputed summary judgment record in this case demonstrates, the government’s policies and practices subject travelers to unfettered searches of their most private digital communications, photographs, and files, untethered from the government’s interest in conducting warrantless searches at the border—namely, to uncover contraband. Petitioners contend that CBP’s and ICE’s policies and practices permitting suspicionless and warrantless searches of electronic devices at the border violate the Fourth Amendment, because such searches must be conducted pursuant to a warrant based on probable cause, or at least an officer’s determination of reasonable suspicion that the device contains digital contraband.

A. Searches of Petitioners

Like the millions of people who cross the U.S. border each year, Petitioners in this case come from all walks of life. They are the editor of a media organization, the operator of a security technology business, a NASA engineer, a journalist, an artist, a filmmaker, a computer programmer, and a university

professor who formerly served as a U.S. Air Force captain. They are U.S. citizens. All were subjected to warrantless searches of their electronic devices at the border. Pet. App. 250a–52a, 157a, 254a–63a (SUMF ¶¶ 124–27, 131–49).¹ None of the Petitioners have been accused of wrongdoing in connection with these border device searches.

Respondents’ searches of Petitioners’ devices were highly invasive. For example, Zainab Merchant had her smartphone searched by CBP officers upon return to the U.S. She wears a headscarf in public in accordance with her religious beliefs, and she objected to male CBP officers searching her device because it contained private images showing her without her headscarf. Pet. App. 258a (SUMF ¶ 139). CBP officers searched Merchant’s phone and asked her questions about her religious affiliation. Pet. App. 257a (SUMF ¶¶ 137–38). When returning to the U.S. from a trip abroad after the filing of this lawsuit, Merchant’s phone was searched again, even though she told the officer that it contained privileged communications with one of her attorneys in this case. Pet. App. 259a–60a (SUMF ¶ 142). Merchant observed a CBP officer reading her communications with her attorney. *Id.* Merchant has been subject to border device searches on four separate occasions. Pet. App. 256–60a (SUMF ¶¶ 136–42).

Isma’il Kushkush, a freelance journalist, had multiple electronic devices searched at Washington

¹ All cites in this brief to “SUMF” refer to Pet. App. 156a–283a, which comprises part of the summary judgment record, namely Plaintiffs’ Reply in Support of Plaintiffs’ Statement of Undisputed Material Facts, ECF No. 99-1; and Plaintiffs’ Supplemental Statement of Undisputed Material Facts, ECF No. 103-1.

Dulles airport. Pet. App. 255a–56a (SUMF ¶¶ 133–35). On a separate occasion when he entered Vermont via bus from Canada, officers searched his smartphone for approximately one hour. Pet. App. 256a (SUMF ¶ 135). Akram Shibly, a filmmaker and graduate student, had his smartphone searched after crossing the land border into New York state. Pet. App. 260a–61a (SUMF ¶¶ 143–44).

Border officers appear to have used special equipment to search the devices of at least three of the Petitioners. Matthew Wright, a computer programmer, had his laptop, smartphone, and digital camera confiscated at the Denver airport. An ICE agent “attempted to image Mr. Wright’s laptop with MacQuisition software, and a CBP forensic scientist extracted data from the SIM card in Wright’s phone and from his camera.” Pet. App. 261a–62a (SUMF ¶¶ 145–47). They also retained the devices, and when a CBP officer told him it might take a year to return them, Wright spent \$2,419.97 for a new laptop and phone, which he needed for work. Pet. App. 270a–71a (SUMF ¶¶ 163–64). His devices were returned after 56 days. Pet. App. 271a (SUMF ¶ 166). When Sidd Bikkannavar, an optical engineer at NASA’s Jet Propulsion Laboratory, arrived in Houston after an international trip, CBP officers searched his smartphone and one officer told him afterward that they had used “algorithms” to do so, Pet. App. 251a–52a (SUMF ¶ 127), which would require using equipment to conduct the search.

Suhaib Allababidi had two smartphones confiscated and sent to the “Regional Computer Forensic Lab” and another location. Pet. App. 268a–69a (SUMF ¶¶ 156–59). The government kept one phone more than two months, and the second more

than ten months. The latter was returned only after the filing of this lawsuit. Pet. App. 269a (SUMF ¶¶ 160–61). Allababidi spent more than \$1,000 on replacement phones. Pet. App. 268a (SUMF ¶ 158).

Three Petitioners were searched on multiple occasions: Merchant, Kushkush, and Allababidi. Pet. App. 250a–51a, 157a, 255a–57a, 259a–60a (SUMF ¶¶ 125, 125.1, 134–35, 137, 140–42). Two were searched after filing the instant lawsuit. Pet. App. 157a, 259a–60a (SUMF ¶¶ 125.1, 140–42). Four had their information retained after border officers searched their devices. Pet. App. 264a (SUMF ¶ 150). The information retained includes descriptions of the contents of Petitioners’ devices. *Id.*

Petitioners travel internationally on a regular basis, and are subject to CBP’s and ICE’s device search policies every time they leave or return to the U.S. Pet. App. 274a–81a (SUMF ¶¶ 169–89). CBP and ICE maintain records of Petitioners’ past searches, and border officers may consult those records when deciding on future device searches, Pet. App. 192a–93a, 196a, 199a–207a, 264a (SUMF ¶¶ 5, 14, 24–51, 150), putting Petitioners at higher risk of repeat searches, as three Petitioners have already experienced. The four Petitioners whose information was unlawfully retained also seek expungement of that information. Pet. App. 264a (SUMF ¶ 150).

B. CBP and ICE Policies and Practices Governing Border Device Searches

CBP and ICE issued border device search policies in 2009 authorizing warrantless and suspicionless searches of electronic devices at the border. Pet. App. 35a. CBP updated its policy in January 2018, Pet. App. 35a–36a, after the filing of

this lawsuit, and several years after the Ninth Circuit’s decision in *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc), which held that border officers must have reasonable suspicion for what the court termed a “forensic” device search using computer equipment to analyze data on a device.

CBP’s currently-operative January 2018 policy (“CBP Policy”) distinguishes between “basic” and “advanced” searches.” Pet. App. 35a–36a. In a basic search, an officer reviews the contents of a device without using external equipment, Pet. App. 164a (SUMF ¶ 8), but is otherwise free to search anything accessible on the device, including by using a device’s internal search tools, Pet. App. 216a (SUMF ¶ 71). In an advanced search, an officer connects external equipment to a traveler’s device to access, review, copy, and/or analyze the contents of the device. Pet. App. 164a (SUMF ¶ 8); Pet. App. 294a (CBP Policy § 5.1.4).

The CBP Policy permits officers to conduct basic searches without any suspicion or other limitation. Pet. App. 195a (SUMF ¶ 10); Pet. App. 293a–94a (CBP Policy § 5.1.3). To conduct an advanced search, the CBP Policy requires “reasonable suspicion of activity in violation of the laws enforced or administered by CBP.” Pet. App. 195a (SUMF ¶ 9); Pet. App. 294a (CBP Policy § 5.1.4). Where officers believe there is a “national security concern,” they may conduct an advanced search without individualized suspicion. Pet. App. 195a (SUMF ¶ 9); Pet. App. 294a (CBP Policy § 5.1.4). In conducting both basic and advanced searches, the CBP Policy prohibits officers from accessing “information that is solely stored remotely.” Pet. App. 293a (CBP Policy § 5.1.2).

However, officers may view information that originated on the internet, such as web-based email, when it has been “cached” on the device, i.e., copied to and still accessible on a device even when disconnected from the internet. Pet. App. 217a (SUMF ¶ 75).

ICE’s border search policy (“ICE Policy”) is governed by a 2009 policy and an ICE Broadcast issued in 2018. Pet. App. 197a (SUMF ¶ 17). Like the CBP Policy, the ICE Policy allows basic searches of electronic devices without any suspicion and advanced searches with reasonable suspicion. Pet. App. 197a (SUMF ¶¶ 18–19).² Both the ICE and CBP policies permit the agencies to retain information related to “immigration, customs, and other enforcement matters,” Pet. App. 196a, 198a–99a (SUMF ¶¶ 13, 22) (citing CBP Policy § 5.5.1.2 and 2009 ICE Policy § 8.5(1)(b)), and to share this information with “federal, state, local, and foreign law enforcement agencies,” Pet. App. 196–99a (SUMF ¶¶ 14, 24).

The frequency of electronic device searches at the border has increased dramatically in recent years. CBP reported searching 40,913 devices in fiscal year 2019,³ an increase of more than 22 percent from fiscal year 2018 (33,295) and up more than 700 percent from fiscal year 2012 (5,085). Pet. App. 207a–08a (SUMF ¶ 52). Because of lapses in record-keeping, these CBP figures are undercounts. *See* Pet. App. 212a–13a

² The ICE Policy does not have a “national security concern” exception to reasonable suspicion for advanced searches. *Compare* Pet. App. 197a (SUMF ¶ 18) *with* Pet. App. 195a (SUMF ¶ 9). *See* Pet. App. 36a.

³ *CBP Statement on Border Search of Electronic Devices* (Oct. 30, 2019), <https://perma.cc/JX8K-BN5B>.

(SUMF ¶¶ 59–62). While ICE conducts hundreds of advanced searches each year, it does not maintain records of basic searches it conducts. Pet. App. 210a–11a (SUMF ¶¶ 56, 58).

The last decade has seen major advances in the storage capacities of electronic devices, as well as in the technological capabilities enabling efficient searches. *See Riley v. California*, 573 U.S. 373, 385 (2014) (recognizing innovations in cell phone technology such that a “smart phone of the sort taken from Riley was unheard of ten years ago”). “Even a basic search alone may reveal a wealth of personal information.” Pet. App. 67a (D. Ct. SMJ Op. at 29) (citing summary judgment record). Electronic devices “can contain a very large volume of information, including . . . prescription information, information about employment, travel history and browsing history.” *Id.* This information “can be accessed during not just the [advanced] searches under the CBP and ICE policies, but also under a basic search.” *Id.* “Using a device’s native operating system, a basic search can access content from the allocated space physically present on the device,” which typically will include personal emails, texts, photographs, health information, personal contacts, and documents. *Id.* A basic search can also “reveal ‘the date/time associated with the content, usage history, sender and receiver information or location data.’” Pet App. 67a–68a. An “agent conducting a basic search may use the device’s own internal search tools to search for particular words or images,” such as doing a keyword search. Pet. App. 68a. Thus, “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.” *Id.*

Respondents conduct warrantless and often suspicionless device searches to gather potential evidence of unlawful conduct with no nexus at all to the admissibility of people and goods. Pet. App. 221a–22a, 226a–27a (SUMF ¶¶ 81–83, 87–88). Respondents assert authority to gather evidence about a wide range of law enforcement matters, including evidence about potential violations of financial, tax, environmental, consumer protection, or other laws—all without a warrant or individualized suspicion. Pet. App. 224a (SUMF ¶ 84). Respondents conduct warrantless, suspicionless searches of electronic devices for intelligence gathering, Pet. App. 225a (SUMF ¶ 86), and search the devices of travelers who are not suspected of any wrongdoing, in order to look for evidence about other people, Pet. App. 228a (SUMF ¶¶ 89–90). Respondents do not know how many warrantless or suspicionless searches of devices uncover digital contraband, or result in arrests, prosecutions, or convictions. Pet. App. 233a (SUMF ¶ 99); *see also* Pet. App. 234a–35a (SUMF ¶¶ 101, 102).

C. Proceedings Below

Petitioners filed suit in September 2017, seeking declaratory and injunctive relief, including expungement of their unlawfully searched and retained information. The district court denied a motion to dismiss, Pet. App. 92a, and then granted in part Petitioners’ motion for summary judgment. Pet. App. 29a. It looked to this Court’s decision in *Riley* for guidance in assessing the significant privacy interests that travelers have in their electronic devices. Pet. App. 62a–66a. In *Riley*, this Court considered the search incident to arrest exception to the Fourth Amendment’s warrant requirement as it applies to

cell phones that can store vast amounts of personal data. The Court recognized that police are generally permitted to search non-digital items on a person incident to arrest without a warrant. But it held that because of the dramatically greater privacy intrusion that a search of a cell phone constitutes, the Fourth Amendment requires a warrant to search a cell phone incident to arrest. *Riley*, 573 U.S. at 401, 403.

The district court reasoned that the border search exception—which, like the search incident to arrest exception, permits certain warrantless (and usually suspicionless) searches—should similarly be modified in light of the greater privacy intrusion that a search of an electronic device constitutes, and the reduced likelihood that an electronic device will contain contraband. The court held that because of the greater privacy concerns raised by searching electronic devices and the reduced government interests given the limited justifications for the border search exception, the Fourth Amendment requires reasonable suspicion that a device contains digital contraband. The court rejected Petitioners’ further argument that such searches require a warrant based on probable cause. Pet. App. 72a–78a.

The court of appeals reversed, holding that Respondents’ policies permitting warrantless and suspicionless searches do not violate the Constitution. The court held that neither probable cause nor a warrant is required for an electronic device search at the border. Pet. App. 17a–19a. It upheld suspicionless “basic” searches, which can include an officer’s perusal of everything on a device. And it also upheld Respondents’ policies authorizing “advanced” searches on reasonable suspicion (and suspicionless advanced searches where there is a “national security

concern”). Pet. App. 18a–21a. The court of appeals also rejected the district court’s conclusion that warrantless device searches at the border must be limited to searching for digital contraband, holding that officers can search for any “violation of the laws enforced or administered by CBP or ICE,” “border-related crime,” “cross-border crime,” or any other “crime at international borders.” Pet. App. 19a–22a.

REASONS FOR GRANTING THE WRIT

I. THE FEDERAL COURTS OF APPEALS ARE DIVIDED ON THE FOURTH AMENDMENT’S REQUIREMENTS FOR BORDER SEARCHES OF ELECTRONIC DEVICES.

Ever since this Court’s 2014 decision in *Riley*, 573 U.S. 373, holding that cell phone searches incident to arrest require a warrant, courts have grappled with how the border search exception applies to searches of electronic devices. The First, Fourth, Ninth, and Eleventh Circuits have each decided some aspect of this question—and none of them agree. The courts of appeals are split on (1) whether and what level of individualized suspicion is required for border searches of electronic devices, and (2) whether warrantless border searches of electronic devices must be limited to searches for digital contraband, or otherwise limited in scope.

As a result, travelers returning home from a trip abroad are subject to different device search rules depending on whether they pass customs at Boston Logan International Airport, San Francisco International Airport, Washington Dulles International Airport, or Hartsfield-Jackson Atlanta

International Airport. People’s Fourth Amendment rights should not vary by the airport they arrive at in the United States. Only this Court can provide the uniform national guidance needed.

A. The Circuits Have Adopted Conflicting Rules on the Permissible Bounds of Border Searches of Electronic Devices.

Four federal courts of appeals have now ruled on how the Fourth Amendment applies to border searches of electronic devices. Each has come up with a different approach.

1. The First Circuit

In the decision below, the First Circuit held that neither a warrant nor probable cause is required for any device search at the border. Pet. App. 16a. It upheld the challenged CBP and ICE policies, which permit basic searches without suspicion, and permit advanced searches “[i]n 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.” Pet. App. 5a, 7a.⁴ And it held that warrantless border device searches need not be limited to searches for digital contraband, but can search for any “violation of the laws enforced or administered by CBP or ICE,” “border-related crime,”

⁴ Petitioners use the terms “basic” and “manual” as well as “advanced” and “forensic” interchangeably here, with the latter two terms referring to electronic device searches involving the connection of external equipment to analyze, review, and/or copy the contents of the device. Petitioners note, however, that some courts upholding a suspicionless manual device search were not examining Respondents’ policies and the meaning and scope of “basic” searches as defined in the CBP and ICE policies. *See, e.g., Cotterman*, 709 F.3d at 960.

“cross-border crime,” or any other “crime at international borders.” Pet. App. 19a–22a.

2. The Ninth Circuit

The Ninth Circuit permits officers to conduct “manual” device searches without individualized suspicion, but requires reasonable suspicion for “forensic” border searches of electronic devices, that is, searches that use separate equipment to search the device. *United States v. Cano*, 934 F.3d 1002, 1016 (9th Cir. 2019), *petition for certiorari pending* (filed Jan. 29, 2021). The *Cano* panel recognized it could not reconsider the rule distinguishing manual and forensic searches that the Ninth Circuit first delineated in *Cotterman*, 709 F.3d 952, an en banc decision that pre-dated *Riley*. *See Cano*, 934 F.3d at 1014–16. The *Cano* court held that all “cell phone searches at the border, whether manual or forensic, must be limited in scope to a search for digital contraband,” and that forensic searches require reasonable suspicion “that the cell phone contains digital contraband.” *Cano*, 934 F.3d at 1007.

3. The Fourth Circuit

The Fourth Circuit held that “some measure of individualized suspicion” is required for forensic searches of electronic devices at the border. *United States v. Kolsuz*, 890 F.3d 133, 137, 144 (4th Cir. 2018).

As to the permissible scope of warrantless device searches, the Fourth Circuit held that there must be a “direct link between the predicate for the search and the rationale for the border exception.” *Id.* at 143. It deemed that link satisfied where border officers sought information about an ongoing transnational crime, namely, illegal firearms exports.

Id. at 143–44. Warrantless searches may be undertaken, the court explained, not only for “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.” *Id.* The Fourth Circuit further refined this rule in *United States v. Aigbekaen*, holding that forensic border searches of electronic devices must “bear[] some nexus to the border search exception’s purposes of protecting national security, collecting duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband.” 943 F.3d 713, 721 (4th Cir. 2019).

The *Aigbekaen* court held that border officers’ search of a device in support of an ongoing domestic criminal investigation was therefore an impermissible use of the border search exception. *Id.* at 721–22. Thus, in the Fourth Circuit, border officers cannot rely on the border search exception, but must “secure a warrant before conducting an intrusive forensic search of a traveler’s digital device, solely to seek evidence of crimes with no transnational component.” *Id.* at 722. The court reasoned that the “[g]overnment may not ‘invoke[] the border exception [to the Fourth Amendment’s warrant requirement] on behalf of its generalized interest in law enforcement and combatting crime.’” *Id.* at 721 (quoting *Kolsuz*, 890 F.3d at 143).

4. The Eleventh Circuit

The Eleventh Circuit has held that “no suspicion is necessary to search electronic devices at the border”—whether forensic or manual. *United States v. Touset*, 890 F.3d 1227, 1229 (11th Cir. 2018); *see also United States v. Vergara*, 884 F.3d 1309,

1311–13 (11th Cir. 2018) (holding that border searches of electronic devices do not require a warrant or probable cause). Nor does it impose any limit on the permissible scope of a border search of an electronic device.

B. The Circuits Are Divided on Whether and What Level of Individualized Suspicion Is Required.

As the summary above illustrates, the courts of appeals are divided on what level of individualized suspicion is required for border device searches. Two circuits, the Fourth and Ninth Circuits, hold that individualized suspicion is required, at least as to forensic searches. *Kolsuz*, 890 F.3d at 137, 140 n.2, 144, 146 n.5; *Cano*, 934 F.3d at 1007; *see also id.* at 1015 n.8 (noting the disagreement between the Eleventh and Ninth Circuit rules). The Eleventh Circuit holds that no individualized suspicion is required for any border device search. *Touset*, 890 F.3d at 1229. And the First Circuit, in the decision below, held that no individualized suspicion is required for basic searches. Pet. App. 4a–5a.

Yet the Fourth Amendment recognizes no distinction between basic and advanced searches. They are distinct only in their method, and both expose vast quantities of highly personal information on an electronic device to the government. Pet. App. 59a–60a (D. Ct. SMJ Op. at 23). This Court in *Riley* required a warrant and probable cause for *any* search of a cell phone incident to arrest—including the manual searches conducted in that case—and drew no distinction based on how the search is done. *See Riley*, 573 U.S. at 379–80, 403.

The courts of appeals are also divided on whether a warrant is ever required. In *Aigbekaen*, the Fourth Circuit held that forensic searches for domestic criminal law enforcement require a warrant. See 943 F.3d at 721–22. The Ninth Circuit requires a warrant where the search seeks anything other than digital contraband. See *Cano*, 934 F.3d at 1007. The First and Eleventh Circuits, by contrast, have rejected a warrant requirement for any border device search. See Pet. App. 16a; *Touset*, 890 F.3d at 1229.

C. The Circuits Are Divided on the Permissible Scope of Warrantless Border Device Searches.

The courts of appeals are also divided on the permissible *scope* of warrantless border searches of electronic devices. The First and Eleventh Circuits have imposed no meaningful limits on the scope of a warrantless device search, while the Fourth and Ninth Circuits have imposed two different scope restrictions. The Ninth Circuit requires that all warrantless device searches be limited to a search for digital contraband. See *Cano*, 934 F.3d at 1007; see also Pet. App. 22a (First Circuit acknowledging that its rejection of a digital contraband limitation is contrary to the Ninth Circuit). The Fourth Circuit agrees that some scope restriction applies, but imposes a different restriction: it requires that forensic border device searches be limited to searches “protecting national security, collecting duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband.” *Aigbekaen*, 943 F.3d at 721. Thus, for the Fourth Circuit, the permissible goals of a border search are not limited to searches for digital contraband itself, but include “the prevention and disruption of ongoing efforts to export

contraband illegally,” *Kolsuz*, 890 F.3d at 143–44. As the *Cano* court acknowledged, “our analysis is in tension with the Fourth Circuit’s decision in *Kolsuz*.” *Cano*, 934 F.3d at 1017.

In short, the courts of appeals are divided along the two principal axes regarding border searches of electronic devices: whether and what level of individualized suspicion is ever required, and whether and how warrantless border searches are limited in their scope. Only this Court can establish a uniform national rule.

II. THIS CASE PRESENTS AN IMPORTANT AND RECURRING QUESTION ON CONSTITUTIONAL PRIVACY RIGHTS IN THE DIGITAL AGE.

Resolution of the question presented is a matter of great importance for the millions of travelers whose privacy rights are at stake every time they cross the border, as well as for the border officers who conduct device searches. At present, four different constitutional regimes govern federal border officials in four different circuits. Device searches at the border are on the rise. And advancing technology increasingly enables individuals to store more personal information on their devices, while empowering government agents to conduct increasingly intrusive searches of those devices. The question presented here is of immediate significance to everyone who crosses our border with a cell phone or other electronic device—and these days, that is virtually every international traveler.

As this Court has explained, pre-digital-age precedents must not be mechanically applied to digital-age searches. *See, e.g., Riley*, 573 U.S. at 386,

400; *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (cell site location data); *United States v. Jones*, 565 U.S. 400 (2012) (GPS transmitter placed on vehicle); cf. *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (thermal imaging device). “As technology has enhanced the Government’s capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to ‘assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’” *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo*, 533 U.S. at 34). Expectations of privacy have traditionally relied on practical limitations on the government’s ability to invade personal privacy; where technological advances have made such invasions “remarkably easy, cheap, and efficient,” greater Fourth Amendment protections are required to maintain privacy. *Id.* at 2217–18; see also *Katz v. United States*, 389 U.S. 347, 362 (1967) (recognizing that Fourth Amendment standards needed to adapt to preserve privacy in the face of advancing wiretapping technology).

This Court has long emphasized, moreover, that any application of exceptions to the Fourth Amendment’s warrant requirement must be closely tethered to the underlying justifications for those exceptions. See *Riley*, 573 U.S. at 386; *Florida v. Royer*, 460 U.S. 491, 500 (1983) (plurality op.) (warrantless searches “must be limited in scope to that which is justified by the particular purposes served by the exception”). Here, as with the exception for searches incident to arrest, application of the border search exception must be reconsidered not only in light of the greatly expanded scale of personal information accessible to border officers through

searches of travelers' electronic devices, but also in light of the limited purposes justifying the border search exception. *See, e.g., United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985) (regulating the collection of duties and preventing the importation of contraband).

Yet lower courts have struggled to assess how the digital revolution affects the border search exception. Today, virtually everyone carries an electronic device that routinely contains more personal information than could be found in their own homes. *See Riley*, 573 U.S. at 396–97. But the analog-era rule that ordinary searches at the border are categorically reasonable without individualized suspicion, adopted when people did not carry anything remotely approaching the amount and kinds of personal information they now carry on electronic devices, renders every traveler vulnerable to revealing a vast array of personal details as a condition of international travel.

Here, as in *Riley*, “innovation[] in surveillance tools” necessitates a re-examination of the historical purposes and protections of the Fourth Amendment. *Carpenter*, 138 S. Ct. at 2214. In the absence of direct guidance from this Court, some lower court judges have felt constrained by analog-era precedents. The Eleventh Circuit simply applied analog-era precedent to border searches of electronic devices, without any adjustment. Judge Jill Pryor, dissenting, would have required a warrant for some border searches of electronic devices, but “[b]ecause *Riley* did not involve a border search,” she could only, “at best, attempt to predict how the Supreme Court would balance the interests here.” *Vergara*, 884 F.3d at 1313 (J. Pryor, J., dissenting). Some district courts would also have

required a warrant for a device search at the border, but felt constrained by pre-*Riley* circuit precedent. See, e.g., *United States v. Caballero*, 178 F. Supp. 3d 1008, 1017–18 (S.D. Cal. 2016) (“If it could, this Court would apply *Riley*.”); *United States v. Molina-Isidoro*, 267 F. Supp. 3d 900, 909 (W.D. Tex. 2016), *aff’d*, 884 F.3d 287 (5th Cir. 2018) (“Were this Court free to decide this matter in the first instance, it might prefer that a warrant be required to search an individual’s cell phone at the border.”).

Given the recurring problems lower courts face in determining the proper application of the Fourth Amendment to electronic device searches at the border, the increasing frequency and intrusiveness of such searches, and the division among the courts of appeals, this Court should resolve the question.

III. THIS CASE IS AN IDEAL VEHICLE TO RESOLVE THESE CONFLICTS.

As noted above, the First Circuit’s decision exacerbates conflicts with respect to both the standard of suspicion required for device searches and the permissible scope of those searches—the two key Fourth Amendment questions that courts have confronted. The posture and facts of this case, unlike other cases involving border searches of electronic devices, would allow this Court to resolve both conflicts on the basis of a developed record generally absent in criminal cases, and in so doing provide guidance for both border officers and the traveling public.

First, this is a civil case in which both the requisite standard of suspicion and the purposes underlying warrantless device searches at the border have been raised, litigated, and decided. Petitioners

have argued for a warrant for all searches of electronic devices at the border, whether basic or advanced, or, in the alternative, an officer's determination of probable cause, or reasonable suspicion of digital contraband for all device searches. Respondents have argued that their policies, which authorize basic searches without suspicion and advanced searches on reasonable suspicion (with no suspicion required for a "national security concern" per the CBP Policy), comply with the Fourth Amendment. The district court decided the Fourth Amendment question on the merits after discovery and cross-motions for summary judgment, and the court of appeals reversed, again on the merits. Thus, all aspects of the Fourth Amendment's application to border searches of electronic devices have been raised and litigated in this case. This includes whether a warrant, probable cause, reasonable suspicion, or no suspicion is required, and whether warrantless border searches must be limited to searching for digital contraband.

Petitioners have standing to raise these questions because they regularly travel internationally with electronic devices and are subject to Respondents' border search policies every time they leave or return to the United States. Indeed, three Petitioners have been searched multiple times, and two after filing this lawsuit. Pet. App. 250a–51a, 157a, 255a–57a, 259a–60a (SUMF ¶¶ 125, 125.1, 134–35, 137, 140–42). And four Petitioners seek expungement of information unlawfully obtained from their searches. Pet. App. 33a–34a.

Second, this case provides a fully developed factual record on summary judgment, establishing critical facts regarding the technological capacities of electronic devices, the amount and breadth of

personal information they contain, and the ease with which that information can be accessed by border officers. These considerations proved decisive in *Riley*, 573 U.S. at 385–86, and here the parties were able to develop a rich evidentiary record on precisely these issues. In the district court, the parties conducted discovery, including document discovery, depositions, and agreeing to factual stipulations. CBP and ICE officials testified regarding Respondents’ purported interests in warrantless and suspicionless border device searches. This fully developed record, which is unlikely to exist in a criminal case, will aid the Court in assessing how the Fourth Amendment should apply to border searches of electronic devices.

Third, the experiences of the Petitioners in this case demonstrate the range of travelers’ privacy interests at stake. Petitioners each have been subjected to searches of their electronic devices at the border. Three had their devices searched multiple times; one traveler was searched four times. Pet. App. 250a–51a, 157a, 255a–57a, 259a–60a (SUMF ¶¶ 125, 125.1, 134–35, 137, 140–42). Two Petitioners were searched both before and after CBP’s and ICE’s adoption of their current policies, and after the filing of this case. Pet. App. 157a, 259a–60a (SUMF ¶¶ 125.1, 140–42). Four Petitioners had their information retained after border officers searched their devices. Pet. App. 264a (SUMF ¶ 150). Petitioners’ devices contained examples of particularly sensitive materials, including private photographs without the headscarf one Petitioner wears in public in accordance with her religious beliefs, Pet. App. 258a (SUMF ¶ 139), and attorney-client privileged communications, Pet. App. 259a–60a (SUMF ¶ 142). Three of the Petitioners whose devices

were searched are media professionals: a journalist, filmmaker, and writer. Pet. App. 255–56a, 260a (SUMF ¶¶ 133, 136, 143). None of the Petitioners have been accused of wrongdoing in connection with their border device searches.

This Court has before it one other petition addressing a subpart of these issues, seeking review of the Ninth Circuit’s decision in *Cano*. See Pet. for a Writ of Cert., *United States v. Cano*, No. 20-1043 (Jan. 29, 2021). *Cano* is a criminal case with a far less robust factual record, and the search in that case took place after the traveler was arrested at the border, which is not the typical fact pattern when border officers search travelers’ devices. Moreover, the question presented in the *Cano* petition addresses only one of the conflicts between the courts of appeals: whether a warrantless border search of an electronic device must be limited to a search for digital contraband. If this Court is inclined to resolve the conflict over the permissible scope of a warrantless border device search, it should also resolve the inextricably inter-related conflict over what standard of suspicion is required, and whether or when warrants are required. Failure to resolve both questions risks continued confusion and inconsistency among the lower courts. This case, in which the district and appellate courts fully considered the Fourth Amendment question, permits the Court to resolve both conflicts.

IV. THE DECISION BELOW IS INCORRECT.

In light of the massive amount of extremely personal information routinely carried on electronic devices today, the Fourth Amendment requires that all searches of electronic devices at the border,

whether basic or advanced, be conducted pursuant to a warrant based on probable cause. At a minimum, it requires that all border device searches be based on reasonable suspicion that the device contains digital contraband. The court of appeals erred in permitting any warrantless border device searches. It also erred in permitting any suspicionless device searches, because all border device searches must be based on at least reasonable suspicion. Lastly, it erred in failing to restrict the scope of warrantless device searches to uncovering digital contraband.

A. The First Circuit Erred in Holding that a Warrant Is Not Required for Electronic Device Searches at the Border.

The First Circuit erroneously held that the Fourth Amendment requires “neither a warrant nor probable cause . . . for a border search of electronic devices.” Pet. App. 16a.

1. *Riley*’s Reasoning Compels a Warrant Requirement for Border Searches of Electronic Devices.

This Court’s reasoning in *Riley* leads to the conclusion that border searches of electronic devices require a warrant. *Cf. Vergara*, 884 F.3d at 1313, 1317–19 (J. Pryor, J., dissenting) (applying *Riley*’s reasoning and concluding that the forensic border search of a cell phone at issue in that case “requires a warrant supported by probable cause”).

As in *Riley*, a consideration of the relevant privacy and governmental interests compels a warrant requirement. Travelers have extraordinary privacy interests in their electronic devices, as the record in this case conclusively shows that they routinely carry devices with vast quantities of highly

personal information, including communications, photographs, browsing history, and contacts that reveal intellectual and political interests, health and financial status, and familial and intimate relations, among other personal details. And the government’s interests in conducting warrantless device searches at the border are as a category weaker than for other warrantless searches because these searches are not sufficiently tethered to the purposes justifying the border search exception: preventing the entry of inadmissible goods and persons. *See, e.g., Montoya de Hernandez*, 473 U.S. at 537. As with the search incident to arrest exception, the border search exception may “strike[] the appropriate balance in the context of physical objects” such as luggage and vehicles, but its underlying rationales lack “much force with respect to digital content on cell phones” or other electronic devices. *Cf. Riley*, 573 U.S. at 386.

a. Privacy Interests in Electronic Devices Are Substantial.

The privacy interests in cell phones and other electronic devices are substantial. The information routinely stored on electronic devices differs qualitatively and quantitatively from that found in luggage and other items typically carried across the border by travelers. *See Riley*, 573 U.S. at 393–94; Pet. App. 214a–18a (SUMF ¶¶ 63–76). The data on electronic devices reveal a detailed account of our thoughts, associations, and interests, whether political, religious, sexual, or romantic. They disclose our financial status, health conditions, and family, professional, and other relationships. *See Riley*, 573 U.S. at 395–96. Irrespective of how they are searched, electronic devices can reveal the “sum of an individual’s private life.” *Id.* at 386. Searches of

electronic devices thus “bear[] little resemblance” to searches of luggage or other containers, *id.*, which are usually “limited by physical realities and tend[] as a general matter to constitute only a narrow intrusion on privacy,” *id.* at 393–94.

b. The Government’s Interests Are Weak Because Electronic Devices Are Unlikely to Contain Contraband.

Border searches of electronic devices also rarely serve the government’s permissible border search interests, because they rarely contain the contraband that the exception was designed to detect. The First Circuit reasoned erroneously that warrantless border searches are justified by purposes as broad as “preventing crime at international borders.” Pet. App. 20a. But this Court’s border search cases have made clear that the limited purposes of the border search exception are customs enforcement—that is, to find and interdict contraband, whether goods smuggled to avoid duties or goods otherwise prohibited from entering the country, *in the items to be searched*—and preventing the entry of inadmissible persons. As discussed further below, even when border officers are searching for digital contraband, Respondents have no valid reason to seek warrantless access to electronic devices.

The scope of the border search exception has always been tied to interdicting contraband and people not entitled to enter. *See Carroll v. United States*, 267 U.S. 132, 154 (1925) (an international traveler may be stopped at the border and required “to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in”); *Montoya de Hernandez*, 473 U.S. at 537

(government may “conduct routine searches and seizures at the border . . . in order to regulate the collection of duties and to prevent the introduction of contraband into this country”); *United States v. 12 200-Ft. Reels of Super 8mm. Film*, 413 U.S. 123, 125 (1973) (discussing the government’s interest in “prevent[ing] smuggling and . . . prohibited articles from entry”); *United States v. Thirty-seven Photographs*, 402 U.S. 363, 376 (1971) (inspecting luggage “is an old practice and is intimately associated with excluding illegal articles from the country”). Yet there is at best a weak nexus between Respondents’ reasons for seeking warrantless access to devices at the border and the limited purposes justifying the border search exception.

First, the record establishes that Respondents conduct warrantless device searches for wide-ranging purposes, including for general law enforcement and intelligence gathering, that are completely untethered from the narrow purposes justifying the border search exception. Pet. App. 221a–24a, 225a–30a (SUMF ¶¶ 82–84, 86–91); *see also Vergara*, 884 F.3d at 1317 (J. Pryor, J., dissenting) (a “general law enforcement justification” does not support warrantless cell phone searches at the border); *City of Indianapolis v. Edmond*, 531 U.S. 32, 42 (2000) (warrantless and suspicionless searches are unreasonable when the “primary purpose . . . is to uncover evidence of ordinary criminal wrongdoing”).

Second, warrantless digital data searches are largely untethered from the primary purpose of the border search exception: interdicting *physical* contraband in the item to be searched. In *Riley*, this Court concluded that warrantless cell phone searches were not sufficiently tethered to the underlying

purposes of the search incident to arrest exception: protecting officer safety and preserving evidence. The Court reasoned, when considering the nexus between warrantless device searches and the specific purpose of uncovering *physical weapons* on an arrestee to protect officer safety, that “data on the phone can endanger no one.” See 573 U.S. at 387. Just as a knife cannot be hidden in digital data, physical contraband cannot be hidden in digital data. By contrast, luggage can contain drugs or other prohibited items. Thus, “the rationales underlying the border search exception lose force when applied to” electronic device searches because electronic devices “do not contain the physical contraband that border searches traditionally have prevented from crossing the border.” See *Vergara*, 884 F.3d at 1317 (J. Pryor, J., dissenting); accord *United States v. Molina-Isidoro*, 884 F.3d at 295 (5th Cir. 2018) (Costa, J., specially concurring) (stating the “detection-of-contraband justification would not seem to apply to an electronic search of a cellphone or computer”).⁵ Respondents argue that they should be permitted to conduct warrantless device searches in order to look for text messages, emails, or other digital evidence *related* to physical contraband smuggling. Yet this purpose is too attenuated from the core purpose of the border search exception: to find dutiable or prohibited goods themselves *in the items to be searched*. See *Molina-Isidoro*, 884 F.3d at 295–96 (Costa, J., specially concurring).

Third, warrantless device searches are not justified even when searching for digital contraband,

⁵ Petitioners do not challenge warrantless border searches of the “physical aspects” of a device, such as a battery compartment, to determine if it contains hidden prohibited items. See *Riley*, 573 U.S. at 387.

for two reasons. The record does not demonstrate that digital contraband is a “prevalent” problem at the border. Pet. App. 233a–34a (SUMF ¶¶ 98–99); *cf. Riley*, 573 U.S. at 389. Digital content that is itself unlawful is rare, *see Cano*, 934 F.3d at 1021 n.13, and child pornography, the most common category of digital contraband, is primarily transported into the United States via the internet, not on electronic devices through ports of entry. Pet. App. 230a (SUMF ¶ 92); *see also* Pet. App. 57a (D. Ct. SMJ Op. at 158) (CBP and ICE proffered a “dearth of information of the prevalence of digital contraband entering the U.S. at the border”). There is also no basis for concluding “that the ability to conduct a warrantless search would make much of a difference” in preventing the importation of digital contraband into the country (or exportation out of the country). *Cf. Riley*, 573 U.S. at 390.⁶ Unlike physical contraband, digital contraband is easily transported across borders via the internet, so travelers have no need or incentive to risk carrying digital contraband on their devices’ hard drives when they cross the border. Pet. App. 230a, 231a–33a (SUMF ¶¶ 92, 95–97); *see also Vergara*, 884 F.3d at 1317 (J. Pryor, J., dissenting) (“[E]lectronic contraband is borderless.”).

Finally, warrantless device searches have virtually no connection to preventing the entry of inadmissible persons, particularly when travelers are U.S. citizens and lawful permanent residents. *See* Pet. App. 75a. (D. Ct. SMJ Op. at 167); Pet. App. 191a–92a

⁶ Respondents do not know how effective warrantless device searches are at preventing the entry of digital files not already present in the United States or uncovering digital contraband in general. Pet. App. 233a–34a (SUMF ¶¶ 98–99).

(SUMF ¶ 2).

Therefore, a categorical rule permitting warrantless border searches of electronic devices is unjustifiable under the Fourth Amendment.

2. This Court Has Left Open the Possibility That Certain Border Searches Require a Warrant.

This Court has never precluded requiring a warrant for a search at the border, nor suggested that reasonable suspicion is a *ceiling*, rather than a floor, for highly intrusive border searches. See *Montoya de Hernandez*, 473 U.S. at 541 n.4 (declining to decide “what level of suspicion” is required for highly intrusive border searches). The Court has contemplated that some border searches may be so unreasonable as to violate the Fourth Amendment, for example, “because of the particularly offensive manner in which [they are] carried out.” *United States v. Flores-Montano*, 541 U.S. 149, 154 n.2 (2004) (quoting *United States v. Ramsey*, 431 U.S. 606, 618 n.13 (1977)). The Court has also left open the possibility that where border searches burden First Amendment rights, the “full panoply” of Fourth Amendment protections—i.e., a warrant—may apply. *Ramsey*, 431 U.S. at 623–24 & n.18.

3. The First Circuit Misconstrued This Court’s Precedent on Warrant Exceptions.

The First Circuit erred by failing to engage with the reasoning in *Riley*. As noted above, the *Riley* Court reexamined the search incident to arrest warrant exception as it applied to the search of cell phones, and found that the nature of cell phone searches required police to obtain a warrant. The Court held that while

prior precedent permitted searches incident to arrest of items on a person without individualized suspicion or a warrant, the dramatically expanded privacy intrusions of cell phone searches and the reduced government interests in searching them without a warrant require a different rule. The same holds true here.

The court of appeals disregarded *Riley* because that case involved warrantless searches incident to arrest, not border searches. Pet. App. 14a. But, as the district court correctly recognized, it is *Riley's analysis* of cell phone searches incident to arrest, not its specific rule, that “is particularly instructive” and “carries persuasive weight” in the border search context. Pet. App. 62a–63a, 134a–35a; *see also Ramsey*, 431 U.S. at 621 (stating that the border search and the search incident to arrest warrant exceptions are “similar”).

The First Circuit also erred in rejecting the rule that warrantless searches “must be limited in scope to that which is justified by the particular purposes served by the exception.” *See* Pet. App. 19a (citing *Royer*, 460 U.S. at 500). The court reasoned that this rule applies only to “non-border contexts” and that “*Riley* did not purport to extend this rule to the border search context.” *Id.* But *Riley's* predicate was that a categorical exception to the Fourth Amendment’s warrant requirement may *not* be applied to a new “category of effects” (such as electronic devices) if doing so would “untether” the exception from its underlying purposes. *Riley*, 573 U.S. at 386; *see also Arizona v. Gant*, 556 U.S. 332, 335 (2009) (refusing to extend the search incident to arrest exception to a warrantless search of a vehicle’s passenger compartment when an individual was arrested near

his car, but without access to it, because there was no reason to believe searching the car would further the interests in protecting officer safety or preventing destruction of evidence); *Collins v. Virginia*, 138 S. Ct. 1663, 1671–72 (2018) (refusing to extend the automobile exception to a warrantless search of a home or its curtilage because doing so would “‘untether’ the automobile exception ‘from the justifications underlying it’”) (quoting *Riley*, 573 U.S. at 386).

B. The First Circuit Erred by Not Holding, in the Alternative, that all Device Searches at the Border Require Reasonable Suspicion that the Device Contains Digital Contraband.

If this Court rejects a warrant requirement, it should at a minimum require an officer determination of reasonable suspicion for all searches of electronic devices at the border, and should limit their permissible scope to finding digital contraband. While not as protective as a warrant requirement, such a rule would partially account for the significant privacy intrusions that searches of electronic devices present, and the substantially reduced likelihood that electronic devices themselves contain contraband. The court of appeals required no suspicion whatsoever for basic searches, and did not limit device searches to a search for digital contraband. Pet. App. 5a.

A requirement that border officers have reasonable suspicion that a device contains digital contraband safeguards travelers’ significant privacy interests in their electronic devices by 1) requiring reasonable suspicion for *all* device searches, irrespective of method, and 2) cabining the scope of

warrantless device searches to looking for digital contraband, consistent with the core purpose of the border search exception: to find and interdict dutiable or prohibited goods *in the items to be searched*. See *supra* Part IV.A.1.b. This rule avoids the gross privacy invasions of international travelers that come with wholly unfettered governmental search authority—where border device searches are conducted without a warrant or any other privacy safeguards.

The rule should apply irrespective of whether the search is “basic” or “advanced” because, as the district court correctly held, and as the record demonstrates, all device searches “implicate the same privacy concerns.” Pet. App. 67a (D. Ct. SMJ Op. at 163). Basic searches can reveal “prescription information, information about employment, travel history and browsing history,” photographs and contact lists, date/time and other metadata. Pet. App. 214a–16a (SUMF ¶¶ 63–71). The searches of Petitioners jeopardized the privacy of private photographs, journalism work product, and attorney-client privileged communications. Pet. App. 257a–58a, 259a–60a (SUMF ¶¶ 138–39, 142). This Court in *Riley* held that *all* searches of a cell phone incident to arrest require a warrant, and did not differentiate between search methods. See *Riley*, 573 U.S. at 403. The searches at issue there were manual. *Id.* at 379–80.

Without a warrant, the appropriate predicate is reasonable suspicion because all border device searches are “non-routine” searches that implicate significant privacy interests, given the vast quantities of highly personal information the government may access at the tap of a finger. See Pet. App. 34a (D. Ct. SMJ Op. at 148). Border searches of electronic devices

do not fall within the traditional border search exception, which permits only “routine” searches to be warrantless and suspicionless, whereas “non-routine” searches require at least reasonable suspicion. *See Montoya de Hernandez*, 473 U.S. at 538; *see also Kolsuz*, 890 F.3d at 137, 144, 145.

Additionally, the reasonable suspicion must be directed to digital *contraband*. In contrast to the Ninth Circuit, which properly imposed this scope limitation, the court of appeals below held that warrantless device searches need not be so limited. It permitted border officers to look for evidence of any “violation of the laws enforced or administered by CBP or ICE,” “border-related crime,” “cross-border crime,” or any other “crime at international borders.” Pet. App. 19a–22a. This wide-ranging approach is contrary to this Court’s precedent, which narrowly defines the purpose of the border search exception and requires that new applications of the exception be sufficiently tethered to this purpose. *See Riley*, 573 U.S. at 386; *Royer*, 460 U.S. at 500.

Therefore, if the Court declines to require a warrant, it should require reasonable suspicion that a device contains digital contraband.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

Adam Schwartz
Sophia Cope
Saira Hussain
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Jessie J. Rossman
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF
MASSACHUSETTS, INC.
211 Congress Street
Boston, MA 02110

Esha Bhandari
Counsel of Record
Hugh Handeyside
Nathan Freed Wessler
Ben Wizner
Hina Shamsi
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street,
New York, NY 10004
(212) 549-2500
ebhandari@aclu.org

David D. Cole
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
915 15th Street, N.W.
Washington, D.C. 20005

Date: April 23, 2021

APPENDIX

APPENDIX A

UNITED STATES COURT OF APPEALS FOR THE FIRST CIRCUIT

Nos. 20-1077

20-1081

GHASSAN ALASAAD; NADIA ALASAAD; SUHAIB
ALLABABIDI; SIDD BIKKANAVAR; 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.

ALEJANDRO MAYORKAS, Secretary of the U.S.
Department of Homeland Security, in his official
capacity;* TROY MILLER, Senior Official Performing
the Duties of the Commissioner of U.S. Customs and
Border Protection, in his official capacity;** TAE D.

* Pursuant to Fed. R. App. P. 43(c)(2), Secretary of the U.S. Department of Homeland Security Alejandro Mayorkas has been substituted for former Acting Secretary of the U.S. Department of Homeland Security Chad F. Wolf as appellant/cross-appellee.

** Pursuant to Fed. R. App. P. 43(c)(2), Senior Official Performing the Duties of the Commissioner of U.S. Customs and Border Protection Troy Miller has been substituted for former Chief Operating Officer and Senior Official Performing the Duties of the Commissioner of U.S. Customs and Border Protection Mark A. Morgan as appellant/cross-appellee.

JOHNSON, Senior Official Performing the Duties of
the Director of U.S. Immigration and Customs
Enforcement, in his official capacity,***

Defendants, Appellants/Cross-Appellees.

APPEALS FROM THE UNITED STATES DISTRICT
COURT FOR THE DISTRICT OF
MASSACHUSETTS

[Hon. Denise J. Casper, U.S. District Judge]

Before

Lynch and Selya, Circuit Judges,
and Laplante,**** District Judge.

Joshua Paul Waldman, Appellate Staff, Civil
Division U.S. Department of Justice, with whom
Joseph H. Hunt, Assistant Attorney General, Scott R.
McIntosh, Appellate Staff, Civil Division U.S.
Department of Justice, and Andrew E. Lelling, United

*** Pursuant to Fed. R. App. P. 43(c)(2), Senior Official
Performing the Duties of the Director of U.S. Immigration and
Customs Enforcement Tae D. Johnson has been substituted for
former Senior Official Performing the Duties of the Director of
U.S. Immigration and Customs Enforcement Tony H. Pham as
appellant/cross-appellee.

**** Of the District of New Hampshire, sitting by
designation.

States Attorney, were on briefs, for appellants/cross-appellees.

Esha Bhandari, with whom Adam Schwartz, Sophia Cope, Saira Hussain, Electronic Frontier Foundation, Hugh Handeyside, Nathan Freed Wessler, American Civil Liberties Union Foundation, Matthew R. Segal, Jessie J. Rossman, and American Civil Liberties Union Foundation of Massachusetts, Inc. were on briefs, for appellees/cross-appellants.

Caroline M. DeCell, Stephanie Krent, Bruce D. Brown, Katie Townsend, Gabriel Rottman, Caitlin Vogus, and Linda Moon on brief for the Knight First Amendment Institute at Columbia University, the Reporters Committee for Freedom of the Press, and 12 Media Organizations, amici curiae.

Kurt Wimmer, Rafael Reyneri, Calvin Cohen, Frank Broomell, and Covington & Burling LLP on brief for the Center for Democracy & Technology, the Brennan Center for Justice, R Street Institute, and Techfreedom, amici curiae.

Michael J. Iacopino, Michael Price, and Mukund Rathi on brief for National Association of Criminal Defense Lawyers, amicus curiae.

Christopher T. Bavitz and Cyberlaw Clinic, Harvard Law School, on brief for Harvard Immigration and Refugee Clinic, amicus curiae.

Meghan Koushik, Mark C. Fleming, Wilmer Cutler Pickering Hale and Dorr LLP, Glenn Katon, and Hammad Alam on brief for Asian Americans Advancing Justice, Asian Law Caucus, et al., amici curiae.

Elizabeth B. Wydra, Brianne J. Gorod, Brian R. Frazelle, and Dayna J. Zolle on brief for Constitutional Accountability Center, amicus curiae.

Jennifer Pinsof, David A. Schulz, Media Freedom & Information Access Clinic, Yale Law School Abrams Institute, Elizabeth A. Ritvo, Joshua P. Dunn, and Brown Rudnick LLP on brief for Floyd Abrams, Jack M. Balkin, Hannah Bloch-Webah, Kiel Brennan-Marquez, Ryan Calo, Danielle Keats Citron, Julie E. Cohen, Catherine Crump, Mary Anne Franks, Woodrow Hartzog, Heidi Kitrosser, Gregory Magarian, Neil M. Richards, Scott Skinner-Thompson, Daniel J. Solove, Amie Stepanovich, Katherine J. Strandburg, and Ari Ezra Waldman, amici curiae.

February 9, 2021

OPINION

LYNCH, Circuit Judge.

Plaintiffs bring a civil action seeking to enjoin current policies which govern searches of electronic devices at this country's borders. They argue that these border search policies violate the Fourth and First Amendments both facially and as applied. The policies each allow border agents to perform "basic" searches of electronic devices without reasonable suspicion and "advanced" searches only with reasonable suspicion. In these cross-appeals we conclude that the challenged border search policies, both on their face and as applied to the two plaintiffs

who were subject to these policies, are within permissible constitutional grounds. We find no violations of either the Fourth Amendment or the First Amendment. While this court apparently is the first circuit court to address these questions in a civil action, several of our sister circuits have addressed similar questions in criminal proceedings prosecuted by the United States. We join the Eleventh Circuit in holding that advanced searches of electronic devices at the border do not require a warrant or probable cause. *United States v. Vergara*, 884 F.3d 1309, 1311-12 (11th Cir. 2018). We also join the Ninth and Eleventh Circuits in holding that basic border searches of electronic devices are routine searches that may be performed without reasonable suspicion. *United States v. Cano*, 934 F.3d 1002, 1016 (9th Cir. 2019), *petition for cert. filed* (Jan. 29, 2021) (No. 20-1043); *United States v. Touse*, 890 F.3d 1227, 1233 (11th Cir. 2018). We also hold the district court erroneously narrowed the scope of permissible searches of such equipment at the border.¹

I. Facts

The material facts are not in dispute. We supplement our description of the facts with the district court's comprehensive statement of facts. *Alasaad v. Nielsen*, 419 F. Supp. 3d 142, 148-50 (D. Mass. 2019); *Alasaad v. Nielsen*, No. 17-cv-11730-DJC, 2018 WL 2170323 at *1-2 (D. Mass. May 9, 2018).

¹ We acknowledge with appreciation the assistance of the amici curiae in this case.

A. Agency Policies

Two policies promulgated by U.S. Customs and Border Protection (“CBP”) and U.S. Immigration and Customs Enforcement (“ICE”) are at issue in this case.

The first policy is CBP Directive No. 3340-049A, Border Search of Electronic Devices (2018), <https://cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf> (the “CBP Policy”). The CBP Policy “provide[s] guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in . . . mobile phones . . . and any other communication, electronic, or digital devices . . . to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer.” CBP Policy at 1.² The CBP Policy defines an “electronic device” as “[a]ny device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players.” *Id.* at 2. The CBP Policy does not address CBP’s authority to search electronic devices with a warrant, consent, or in response to exigent circumstances. *Id.*

The CBP Policy distinguishes between “basic” and “advanced” searches.³ It defines an “advanced search” as “any search in which an Officer connects

² The Policy is mandatory. CBP Policy at 1 (“All CBP Officers . . . *shall* adhere to the policy.” (emphasis added)).

³ “Advanced” searches are sometimes referred to as “forensic” searches. Through the terms are not precisely co-extensive, any difference is immaterial here.

external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents.” *Id.* at 5. Advanced searches require “supervisory approval” and under the CBP Policy may only be performed “[i]n 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.” *Id.* A “basic search” is any non-advanced search. *Id.* at 4. The CBP Policy states that a basic search may be performed “with or without suspicion.” *Id.*

For both basic and advanced searches, the CBP Policy only allows officers to search “information that is resident upon the device,” and devices must be disconnected from the internet before a search is performed. *Id.*

In addition, the CBP Policy states that “[a]n Officer may detain electronic devices . . . for a brief, reasonable period of time to perform a thorough border search.” *Id.* at 7.

The second policy is Immigration and Customs Enforcement Directive No. 7-6.1, Border Searches of Electronic Devices (2009), https://hdhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf, (“ICE Directive”) as superseded in part by *Immigration and Customs Enforcement Broadcast: Legal Update — Border Search of Electronic Devices* (2018) (“ICE Broadcast”), (together “ICE Policy” and, together with the CBP Policy, the “Policies”). The ICE Policy governs ICE’s searches of electronic devices at the border “to ensure compliance with customs, immigration, and other laws enforced by ICE.” ICE Directive at 1. The policy defines an

“electronic device” as “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.” ICE Directive at 2. The policy allows for suspicionless basic searches but states that as of May 11, 2018, ICE agents “should no longer perform advanced border searches of electronic devices without reasonable suspicion.” ICE Broadcast. The ICE Policy also allows agents to detain electronic devices for a “reasonable time given the facts and circumstances of the particular search.” ICE Directive at 4.

Plaintiffs do not argue there are any meaningful differences between the two agencies’ policies.

B. The Searches of Plaintiffs’ Electronic Devices

Plaintiffs are ten U.S. citizens and one lawful permanent resident. Each states that CBP or ICE officers searched his or her electronic devices on one or more occasions.

Only plaintiffs Zainab Merchant and Suhaib Allababidi allege that they were searched after CBP issued its revised 2018 policy and ICE published its advanced search policy. These searches were basic searches. These two plaintiffs do not allege that their devices were retained pursuant to the Policies. Accordingly, no factual information has been presented to us as to any detention under these policies.

II. Procedural History

Plaintiffs filed suit on September 13, 2017 — before the effective date of the challenged Policies — alleging that CBP and ICE violated the Fourth and First Amendments by performing various types of searches of electronic devices without warrants and violated the Fourth Amendment by retaining plaintiffs’ electronic devices for an extended period absent probable cause.⁴ The plaintiffs sought declaratory and injunctive relief, including expungement of “all information gathered from, or copies made of, the contents of Plaintiffs’ electronic devices.”

On May 9, 2018, the district court denied the government’s motion to dismiss. *Alasaad*, 2018 WL 2170323 at *24.

After discovery, the parties filed cross-motions for summary judgment. The district court granted in part and denied in part plaintiffs’ motion for summary judgment and denied the government’s motion for summary judgment. *Alasaad*, 419 F. Supp. 3d at 174. The district court also held that plaintiffs had standing to seek declaratory and injunctive relief as

⁴ No plaintiff in this case asserts that his or her electronic device passcodes or passwords were entitled to additional constitutional protections.

A petition for a writ of certiorari is pending before the Supreme Court in *Andrews v. New Jersey* as to whether the Fifth Amendment protects an individual from being compelled to disclose the passcodes to his or her electronic devices when doing so may expose the individual to criminal prosecution. Petition for Writ of Certiorari, *Andrews v. New Jersey*, (No. 20-937).

well as expungement of their data from CBP and ICE databases. *Id.* at 151-54.⁵

As to the merits of the Fourth Amendment challenges, the district court first held that basic and advanced searches are both “non-routine” searches, and thus that both types of searches required reasonable suspicion.⁶ *Id.* at 163, 165. The court concluded that the basic search component of the Policies violated the Fourth Amendment. *Id.* at 165, 168.

As to the scope of both basic and advanced searches permitted under the Policies, the court found two constitutional violations. It reasoned that because the border search exception is premised on the government’s paramount interest in “stopping contraband at the border,” “the reasonable suspicion that is required . . . is . . . that the electronic devices contain[] contraband [itself],” rather than (a) *evidence* of contraband or (b) evidence or information regarding other crimes enforced at the border. *Id.* at 166. Thus, the Policies were unconstitutional because they did not restrict agents to searches for contraband contained in the devices themselves and allowed border searches as to evidence of all crimes CBP or

⁵ The government does not challenge plaintiffs’ standing on appeal.

⁶ The district court noted 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 . . . [would] not require a heightened showing of cause.” *Alasaad*, 419 F. Supp. 3d at 163.

ICE are authorized to enforce.⁷ CBP Policy at 1, 5; ICE Directive at 1, 2.

As to the long-term detention of plaintiffs' electronic devices, the district court held that devices detained based on reasonable suspicion could be retained only for a "reasonable period that allows for an investigatory search for contraband." *Alasaad*, 419 F. Supp. 3d at 170.

The district court granted declaratory relief stating that

the CBP and ICE policies for "basic" and "advanced" searches . . . 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.

Id. at 173.

⁷ ICE and CBP are authorized to enforce a broad spectrum of laws. *See, e.g.*, 6 U.S.C. § 211(c)(5) (requiring CBP to "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"); *id.* § 211(c)(11) (requiring CBP to "enforce and administer the laws relating to agricultural import"); 31 U.S.C. §§ 5316-17 (authorizing warrantless border searches to enforce limitations on transferring \$10,000 or more out of the United States); 19 C.F.R. § 12.39 (authorizing CBP to enforce law restricting the importation of "articles involving unfair methods of competition").

The district court declined to grant broad injunctive relief based on its finding of constitutional violations. *Id.* at 174. It did enjoin the government from searching or detaining any of plaintiffs’ electronic devices at the border absent “reasonable suspicion that the device contains contraband,” and from detaining plaintiffs’ electronic devices for “longer than a reasonable period.”

The district court denied plaintiffs’ request for expungement. *Id.* at 171-73.

As to the First Amendment claim, the district court did not analyze that claim independently from the Fourth Amendment claim. It denied plaintiffs’ claim for relief, saying “to the extent that [the First Amendment claim] seeks some further ruling or relief based upon Plaintiffs’ invocation of First Amendment rights, not otherwise granted as to [plaintiffs’ Fourth Amendment claim],” it would deny plaintiffs’ motion for summary judgment. *Id.* at 170.

The government filed a timely notice of appeal, and plaintiffs cross-appealed.

III. Analysis

We review a grant of summary judgment de novo. *Henderson v. Mass. Bay Transp. Auth.*, 977 F.3d 20, 29 (1st Cir. 2020). “Cross-motions for summary judgement do not alter the basic . . . standard, but rather simply require us 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. Ferre Dev., Inc.*, 241 F.3d 103, 107 (1st Cir. 2001).

We begin with plaintiffs’ Fourth Amendment claims before moving to their First Amendment claim and request for expungement.

A. The Level of Suspicion Required for Border Searches of Electronic Devices

Plaintiffs argue that all electronic device searches at the border require a warrant, or in the alternative that such searches require reasonable suspicion that the device contains contraband. Plaintiffs do not contest that the Policies require ICE and CBP to have reasonable suspicion to perform an advanced border search. We address the arguments in turn.

1. Border Searches of Electronic Devices Do Not Require a Warrant

The Fourth Amendment forbids “unreasonable searches and seizures.” U.S. Const. amend. IV. “In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.” *Riley v. California*, 573 U.S. 373, 382 (2014). Otherwise,

[a]bsent more precise guidance from the founding era, we generally determine whether to exempt a given type of search 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.”

Id. at 385 (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)).

One such exception to the warrant requirement, recognized from early in our history, is the border search exception. See *Boyd v. United States*, 116 U.S. 616, 623 (1886); *Carroll v. United States*, 267 U.S. 132, 153-54 (1925). The exception is grounded in the government’s “inherent authority to protect, and a paramount interest in protecting, its territorial integrity.” *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). Further, “the 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 also struck much more favorably to the Government at the border.” *United States v. Montoya de Hernandez*, 473 U.S. 531, 539-40 (1985).

Plaintiffs rely on *Riley v. California* to argue that the border search warrant exception does not encompass the search of electronic devices because such searches do little to advance the underlying purposes of the border search exception — which they say are limited to interdicting contraband and preventing the entry of inadmissible persons.⁸

This argument rests on a misapprehension of the applicability here of the Supreme Court’s holding in *Riley*. In *Riley*, the Supreme Court held that the search incident to arrest exception to the warrant requirement did not extend to searches of cellphones. 573 U.S. at 403. In doing so, it reasoned that individuals have a heightened privacy interest in their electronic devices due to the vast quantity of data that may be stored on such devices, and that the

⁸ For reasons articulated later in this opinion, we reject plaintiffs’ narrow view of the purposes of the border search exception.

government's interest in searching an arrestee's cellphone during an arrest was limited because such searches do not meaningfully advance the search incident to arrest exception's purposes of protecting officers and preventing the destruction of evidence. *Id.* at 386, 388-91. Thus, the balance of interests did not support extending the search incident to arrest exception. *Id.* at 386.

Contrary to plaintiffs' assertions, *Riley* does not command a warrant requirement for border searches of electronic devices nor does the logic behind *Riley* compel us to impose one. As recently explained by this circuit, *Riley* “d[id] not either create or suggest a categorical rule to the effect that the government must always secure a warrant before accessing the contents of [an electronic device].” *United States v. Rivera-Morales*, 961 F.3d 1, 14 (1st Cir. 2020). Nor does *Riley* by its own terms apply to border searches, which are entirely separate from the search incident to arrest searches discussed in *Riley*. The search incident to arrest warrant exception is premised on protecting officers and preventing evidence destruction, rather than on addressing border crime. *Riley*, 573 U.S. at 384-86.

Further, given the volume of travelers passing through our nation's borders, warrantless electronic device searches are essential to the border search exception's purpose of ensuring that the executive branch can adequately protect the border. *See Montoya de Hernandez*, 473 U.S. at 544 (stating that border officials are “charged . . . with protecting this Nation from entrants who may bring anything harmful into this country”). A warrant requirement — and the delays it would incur — would hamstring the

agencies' efforts to prevent border-related crime and protect this country from national security threats.

Every circuit that has faced this question has agreed that *Riley* does not mandate a warrant requirement for border searches of electronic devices, whether basic or advanced. The Eleventh Circuit held that “[b]order searches have long been excepted from warrant and probable cause requirements, and the holding of *Riley* does not change this rule.” *Vergara*, 884 F.3d at 1312-13. The Fourth Circuit held after *Riley* that “law enforcement officers may conduct a warrantless forensic search of a cell phone under the border search exception where the officers possess sufficient individualized suspicion of transnational criminal activity.” *United States v. Aigbekaen*, 943 F.3d 713, 719 n.4 (4th Cir. 2019).⁹ The Ninth Circuit, noting that even “post-*Riley*, no court has required more than reasonable suspicion to justify even an intrusive border search,” held that both basic and advanced border searches may be performed without a warrant or probable cause. *Cano*, 934 F.3d at 1015-16.

We too hold that neither a warrant nor probable cause is required for a border search of electronic devices.

2. *Basic Searches May Be Performed Without Reasonable Suspicion*

Agents may perform “routine” searches at the border without reasonable suspicion. *Montoya de Hernandez*, 473 U.S. at 538, 541. Under this circuit’s

⁹ The Fourth Circuit did not decide whether an advanced search must be supported by probable cause. *Aigbekaen*, 943 F.3d at 720 & n.5.

law, certain “non-routine” searches must be grounded on reasonable suspicion. *United States v. Molina-Gómez*, 781 F.3d 13, 19 (1st Cir. 2015); *United States v. Braks*, 842 F.2d 509, 513-14 (1st Cir. 1988). Whether a border search is routine or non-routine depends on an assessment of the facts of the case. *Braks*, 842 F.2d at 512 (holding that request to female at border to lift skirt was routine search); *Molina-Gómez*, 781 F.3d at 19 (holding that the search of a laptop and PlayStation, whether routine or non-routine, was justified because reasonable suspicion existed); *United States v. Robles*, 45 F.3d 1, 5 (1st Cir. 1995) (holding, where the government conceded that drilling into metal cylinder was non-routine search, that the search was justified by reasonable suspicion). Subjecting individuals to strip searches or body-cavity searches are examples of non-routine searches. *Molina-Gómez*, 781 F.3d at 19.

Plaintiffs argue that because electronic devices may contain a trove of sensitive personal information, basic border searches of electronic devices are non-routine searches requiring at least reasonable suspicion. While, as noted above, *Riley*’s warrant requirement in the search incident to arrest context does not extend to border searches, *Riley* recognized that modern electronic devices “implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse” and “differ in both a quantitative and qualitative sense from other objects that might be kept on [a traveler’s] person.” 573 U.S. at 393. These privacy concerns, however significant or novel, are nevertheless tempered by the fact that the searches are taking place at the border, where the “Government’s interest in preventing the

entry of unwanted persons and effects is at its zenith,” *Flores-Montano*, 541 U.S. at 152, and the “Fourth Amendment balance of interests leans heavily to the Government,” *Montoya de Hernandez*, 473 U.S. at 544. Electronic device searches do not fit neatly into other categories of property searches, but the bottom line is that basic border searches of electronic devices do not involve an intrusive search of a *person*, like the search the Supreme Court held to be non-routine in *Montoya de Hernandez*. 473 U.S. at 541 & n.4. Basic border searches also require an officer to manually traverse the contents of the traveler’s electronic device, limiting in practice the quantity of information available during a basic search. The CBP Policy only allows searches of data resident on the device. CBP Policy at 4. And a basic border search does not allow government officials to view deleted or encrypted files.¹⁰

We thus agree with the holdings of the Ninth and Eleventh circuits that basic border searches are routine searches and need not be supported by reasonable suspicion. *Cano*, 934 F.3d at 1016; *Touset*, 890 F.3d at 1233; *see also United States v. Kolsuz*, 890 F.3d 133, 146 n.5 (4th Cir. 2018) (stating that *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005) “treated a [basic] search of a computer as a routine border

¹⁰ Plaintiffs argue that because a basic border search can take place over an extended period, “the policies place no limit on the scope of a basic search.” This claim is not supported by the record. As laid out in the complaint, basic searches are limited to “allocated space physically resident on an electronic device that is accessible using the native operating system of the device.” And the agencies must process the entry of over one million travelers per day, further restricting the practical limits of a basic search.

search, requiring no individualized suspicion for the search”).

B. The Scope of Searches Permitted under the Border Search Exception

Plaintiffs next argue that border searches of electronic devices “must be limited to searches for contraband.” This argument is premised on plaintiffs’ assertions that the border search exception (a) extends only to searches aimed at preventing the importation of contraband or entry of inadmissible persons and (b) covers only searches for contraband itself, rather than for *evidence* of border-related crimes or contraband. The argument fails and its premises are incorrect.

In non-border contexts the Supreme Court has held that warrantless searches “must be limited in scope to that which is justified by the particular purposes served by the exception.” *Florida v. Royer*, 460 U.S. 491, 500 (1983) (plurality opinion); *see also Riley*, 573 U.S. at 386. *Riley* did not purport to extend this rule to the border search context. Even assuming *arguendo* that the analysis used in *Riley* applies here, such an analysis would only require that warrantless border searches be tethered to “the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country.”¹¹ *Flores-Montano*, 541 U.S. at 152 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)). Further, the Supreme Court has repeatedly said that routine searches “are reasonable simply by virtue of

¹¹ Plaintiffs do not challenge any specific law enforced by CBP or ICE as having no relationship to the border search exception’s broad purposes.

the fact that they occur at the border.” *Id.* at 152-53 (quoting *Ramsey*, 431 U.S. at 616). This is so because the government’s interest in preventing crime at international borders “is at its zenith,” *see id.*, and it follows that a search for evidence of either contraband or a cross-border crime furthers the purposes of the border search exception to the warrant requirement.

As for advanced searches, we cannot reasonably conclude that the “substantive limitations imposed by the Constitution” on the border search exception prevent Congress from giving border agencies authority to search for information or items other than contraband. *Ramsey*, 431 U.S. at 620; *see also Kolsuz*, 890 F.3d at 152 (Wilkinson, J., concurring in the judgment) (“[T]here is a longstanding historical practice in border searches of deferring to the legislative and executive branches.”). To the contrary, *Montoya de Hernandez* makes clear that the border search exception’s purpose is not limited to interdicting contraband; it serves to bar entry to those “who may bring *anything* harmful into this country” and then gives as examples “whether that be communicable diseases, narcotics, or explosives.” 473 U.S. at 544.

Congress is better situated than the judiciary to identify the harms that threaten us at the border.¹²

¹² As explained by Judge Wilkinson, “[w]e have no idea of the dangers we are courting” at the border. *Kolsuz*, 890 F.3d at 152 (Wilkinson, J., concurring in the judgment). He notes the risk that “[p]orous borders are uniquely tempting to those intent upon inflicting the vivid horrors of mass casualties” and “the danger of highly classified technical information being smuggled out of this country only to go into the hands of foreign nations who do not wish us well and who seek to build their armaments to an ever more perilous state.” *Id.*

Kolsuz, 890 F.3d at 152 (Wilkinson, J, concurring in the judgment) (“[*Riley* does not] begin to answer the question of *who* should strike the balance between privacy and security at the border of the country.”); *see also Riley*, 573 U.S. at 408 (Alito, J., concurring in part and concurring in the judgment) (stating with respect to the reasonableness of warrantless searches of mobile phones that “[l]egislatures . . . are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future”). In weighing the competing policy considerations, Congress or the Executive may choose to strike a different balance as to border searches of electronic devices and may choose to grant greater protection than required by the Constitution.

As to plaintiffs’ distinction between evidence of contraband and contraband itself, the border search exception is not limited to searches for contraband itself rather than evidence of contraband or a border-related crime. Searching for evidence is vital to achieving the border search exception’s purposes of controlling “who and what may enter the country.” *Ramsey*, 431 U.S. at 620; *see also Aigbekaen*, 943 F.3d at 721 (holding that the purposes of the border search exception are “protecting national security, collecting duties, blocking the entry of unwanted persons, [and] *disrupting efforts to export or import contraband*” (emphasis added)); *United States v. Gurr*, 471 F.3d 144, 149 (D.C. Cir. 2006) (holding in the context of the border search exception that “[t]he distinction that [plaintiff] would draw between contraband and

documentary evidence of a crime is without legal basis”).¹³

We acknowledge that our holdings on both of these points are contrary to the Ninth Circuit’s holdings in *United States v. Cano*. 934 F.3d at 1018 (holding that the border search exception “is restricted in scope to searches for contraband”). We cannot agree with its narrow view of the border search exception because *Cano* fails to appreciate the full range of justifications for the border search exception beyond the prevention of contraband itself entering the country. Advanced border searches of electronic devices may be used to search for contraband, evidence of contraband, or for evidence of activity in violation of the laws enforced or administered by CBP or ICE.

C. Device Detention

Plaintiffs further argue that the CBP and ICE Policies violate the Fourth Amendment because they

¹³ Plaintiffs cite *Boyd*, 116 U.S. 616, for the proposition that the border search exception does not extend to searching for evidence of border-related crimes. But the Supreme Court rejected in *Warden, Md. Penitentiary v. Hayden* the distinction articulated in *Boyd* between searches for “mere evidence” and searches for “instrumentalities, fruits of crime, or contraband.” 387 U.S. 294, 301 (1967). Plaintiffs argue that *Hayden* only rejected this distinction in relation to searches authorized by a warrant rather than warrantless searches, but we conclude that *Hayden* should be more broadly applied. See *United States v. Molina-Isidoro*, 884 F.3d 287, 297 n.7 (5th Cir. 2018) (Costa, J., specially concurring) (“*Hayden* is viewed as a broad rejection of the ‘mere evidence’/instrumentality distinction” (citing Wayne LaFave, *Search & Seizure, A Treatise on the Fourth Amendment* § 4.1(c))). But see *id.* (“[T]here are reasons to believe the [mere evidence/instrumentality] distinction still matters when it comes to border searches.”).

do not impose an “effective limit on [the] duration” of electronic device detentions.¹⁴ Plaintiffs’ argument is in the abstract as they have not presented any facts concerning the actual retention of devices pursuant to the policies at issue.

The CBP Policy permits an officer to “detain electronic devices or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search.” CBP Policy at 7. Supervisory approval is required to detain devices after the device owners “departure from the port or other location of detention.” *Id.* The ICE Policy permits the detention of “electronic devices, or copies of information therefrom [for] a reasonable time given the facts and circumstances of the particular search.” ICE Directive at 4. Both Policies require supervisory approval to extend a device detention beyond an initial span of time — five days under the CBP Policy and thirty days under the ICE policy. CBP Policy at 7; ICE Directive at 5.

The nature of plaintiffs’ challenge is unclear. The Policies permit detention for only a reasonable period, which is the constitutional test. *See Montoya de Hernandez*, 473 U.S. at 544. If the argument is that “reasonable” must be replaced with hard time limits, the Supreme Court has rejected that proposition. *Id.* at 543. If the argument is that the judgment as to reasonableness should not be left in the first instance to the agent who conducts the search, that misreads

¹⁴ Because we conclude that no reasonable suspicion is required for a basic border search of an electronic device, we need not reach plaintiffs’ contention that the Policies are deficient in allowing the agencies to detain devices without reasonable suspicion.

the Policies. The CBP Policy requires a supervisor's permission to detain a device after its owner leaves the border, a higher level of supervisory approval to extend a detention for longer than five days, and a third level of approval to extend a detention beyond fifteen days. CBP Policy at 7. What is reasonable is surely fact specific and future as applied attacks are not foreclosed should there be abuses.¹⁵

D. First Amendment

Plaintiffs next argue that under the First Amendment, government searches of electronic devices at the border require a warrant, or at least reasonable suspicion. They contend that because electronic devices may contain sensitive personal data, the threat of warrantless or suspicionless border searches will impermissibly chill speech.¹⁶ They

¹⁵ Plaintiffs do not develop the argument that any individual detention of any plaintiff's electronic device was unreasonable, but instead say that several particularly long detentions demonstrate that the Policies are facially deficient.

¹⁶ Plaintiffs purport to rely on *United States v. Ramsey*, 431 U.S. 606 (1977), but misunderstand the case. In *Ramsey*, plaintiffs argued that the search of international mail was a violation of the First Amendment. The applicable law allowed the search of international mail only where there was "reasonable cause to believe" that customs laws [were] being violated prior to the opening of envelopes" and a regulation forbade the "reading of *correspondence* absent a search warrant." *Id.* at 623 (emphasis added). The Supreme Court held that under those circumstances, the opening of international mail did not "impermissibly chill[] the exercise of free speech." *Id.* at 624.

The court explicitly reserved and did not decide the question of whether the search of international mail, "in the absence of the regulatory restrictions" would chill speech and, if it did, "whether the appropriate response would be to apply the full panoply of Fourth Amendment requirements." *Id.* at 624 n.18.

further argue that such searches unduly interfere with the First Amendment freedoms to “engage in association’ . . . without government scrutiny, . . . speak anonymously, . . . receive unpopular ideas, confidentially and without government scrutiny, . . . read books and watch movies privately . . . [and] gather and publish newsworthy information absent government scrutiny.”

Because plaintiffs seek relief “beyond [their] particular circumstances,” “they must ‘satisfy [the] standards for a facial challenge to the extent of that reach.’” *Proj. Veritas Action Fund v. Rollins*, 982 F.3d 813, 826 (1st Cir. 2020) (emphasis omitted) (quoting *John Doe No. 1 v. Reed*, 561 U.S. 186, 194 (2010)). Thus, plaintiffs must show that “a substantial number of [the ICE and CBP Policies] applications are unconstitutional, judged in relation to the statute’s plainly legitimate sweep.” *United States v. Stevens*, 559 U.S. 460, 473 (2010) (quoting *Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 449 n.6 (2008)).

The First Amendment provides protections — independent of the Fourth Amendment — against the compelled disclosure of expressive information. See *Buckley v. Valeo*, 424 U.S. 1, 64 (1976); *Tabbaa v. Chertoff*, 509 F.3d 89, 102 n.4 (2d Cir. 2007) (analyzing First Amendment challenge to targeted border searches independently of Fourth Amendment); *Ramsey*, 431 U.S. at 623-24. Neither this circuit nor the Supreme Court has specified the appropriate standard to assess alleged government intrusions on First Amendment rights at the border. See *Ramsey*, 431 U.S. at 623-24 (refusing to “consider the constitutional reach of the First Amendment in this

area”); *see also* *Tabbaa*, 509 F.3d at 102 n.5 (“It may also be true that the First Amendment’s balance of interests is qualitatively different where, as here, the action being challenged is the government’s attempt to exercise its broad authority to control who and what enters the country.”).

Under any standard plaintiffs have not shown that the content-neutral border search Policies facially violate the First Amendment. *See Ramsey*, 431 U.S. at 623 (“More fundamentally, however, the existing system of border searches has not been shown to invade protected First Amendment rights, and hence there is no reason to think that the potential presence of correspondence makes the otherwise constitutionally reasonable search ‘unreasonable.’” (footnote omitted)). The Policies have a plainly legitimate sweep and serve the government’s paramount interests in protecting the border.¹⁷

Nor, as plaintiffs contend, does the presence of expressive material on electronic devices “trigger[] a warrant requirement.” A higher level of suspicion is not generally required to search potentially expressive materials. *See New York v. P.J. Video, Inc.*, 475 U.S. 868, 875 (1986); *United States v. Brunette*, 256 F.3d 14, 16 (1st Cir. 2001) (holding the probable cause

¹⁷ Plaintiffs do not present the issue of whether the First Amendment would require a different outcome if CBP and ICE were targeting journalists or using border searches to pierce attorney-client privilege. Two plaintiffs are journalists, but they do not contend that they were searched by CBP for this reason. *See Alasaad*, 419 F. Supp. 3d at 169. This decision does not foreclose a future as applied First Amendment challenge in such circumstances. *See Ortiz-Graulau v. United States*, 756 F.3d 12, 21 (1st Cir. 2014) (noting that this court may leave open “the possibility of a future as-applied challenge”).

standard “is no different where First Amendment concerns may be at issue”); *see also Ickes*, 393 F.3d at 507 (refusing to apply a different standard to border searches of expressive material); *United States v. Arnold*, 533 F.3d 1003, 1010 (9th Cir. 2008) (same).

As explained by the Ninth Circuit in *Arnold*, providing a different standard for “expressive material” at the border would

(1) protect terrorist communications “which are inherently ‘expressive’”; (2) create an unworkable standard for government agents who “would have to decide — on their feet — which expressive material is covered by the First Amendment”; and (3) contravene the weight of Supreme Court precedent refusing to subject government action to greater scrutiny with respect to the Fourth Amendment when an alleged First Amendment interest is also at stake.

533 F.3d at 1010 (quoting *Ickes*, 393 F.3d at 506). Plaintiffs’ First Amendment challenge fails.

E. Expungement

Plaintiffs argue they are entitled to expungement of any data obtained in violation of the Constitution. The district court’s refusal to grant the equitable remedy of expungement is reviewed only for abuse of discretion. *Reyes v. DEA*, 834 F.2d 1093, 1098-99 (1st Cir. 1987).

There was no abuse of discretion here. The district court adequately justified its conclusions that expungement was not warranted. And contrary to plaintiffs’ assertions, it was not error for the district

court to analogize to caselaw regarding the suppression of evidence.

IV. Conclusion

We *affirm* in part, *reverse* in part, *vacate* in part, and *remand* for the entry of a revised judgment consistent with this opinion. No costs imposed.

APPENDIX B

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

No. 17-cv-11730-DJC

GHASSAN ALASAAD, NADIA ALASAAD, SUHAIB
ALLABABIDI, SIDDIKANNANAVAR, 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.

November 21, 2019

JUDGMENT

CASPER, J.

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

APPENDIX C

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

No. 17-cv-11730-DJC

GHASSAN ALASAAD, NADIA ALASAAD, SUHAIB
ALLABABIDI, SIDD BIKKANAVAR, 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.

November 12, 2019

MEMORANDUM AND ORDER

CASPER, J.

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

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.

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 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, 126, 128, 131, 133, 136, 143, 145, 148; D. 99-1 at ¶¶ 120, 124, 126, 128, 131, 133, 136, 143, 145,

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.

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 Plaintiffs 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 ¶¶ 25-51. Accordingly, such Plaintiffs have standing to seek expungement, even as the Court reserves for

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

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).

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))).

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.

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 protect[ing] 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. Tousef*, 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,

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

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 once identity and citizenship are established); *cf.* 8 U.S.C. § 1225 (providing that an

still be available even as it ruled that a warrantless search of cell phone was not permissible as a search incident to arrest).

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

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.

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 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 suspicion⁷ in the border context have already been laid by several

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

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 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

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”).

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 investigatory 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 information⁹ 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

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.

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 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

APPENDIX D

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

No. 17-cv-11730-DJC

GHASSAN ALASAAD, NADIA ALASAAD, SUHAIB
ALLABABIDI, SIDD BIKKANAVAR, JÉRÉMIE
DUPIN, AARON GACH, ISMAIL ABDEL-RASOUL
a/k/a ISMA'IL KUSHKUSH, DIANE MAYE, ZAINAB
MERCHANT, MOHAMMED AKRAM SHIBLY and
MATTHEW WRIGHT,

Plaintiffs,

v.

KIRSTJEN NIELSEN, Secretary of the U.S.
Department of Homeland Security, in her official
capacity; KEVIN McALEENAN, Acting
Commissioner of U.S. Customs and Border
Protection, in his official capacity; and THOMAS
HOMAN, Acting Director of U.S. Immigration and
Customs Enforcement, in his official capacity,

Defendants.

May 9, 2018

MEMORANDUM AND ORDER

CASPER, J.

I. Introduction

Plaintiffs Ghassan Alasaad, Nadia Alasaad, Suhaib Allababidi (“Allababidi”), Sidd Bikkannavar (“Bikkannavar”), Jérémie Dupin (“Dupin”), Aaron Gach (“Gach”), Ismail Abdel-Rasoul a/k/a Isma’il Kushkush (“Kushkush”), Diane Maye (“Maye”), Zainab Merchant (“Merchant”), Mohammed Akram Shibly (“Shibly”) and Matthew Wright (“Wright”) (collectively, “Plaintiffs”) bring this suit against the following persons in their official capacities: Kirstjen Nielsen (“Nielsen”), Secretary of the U.S. Department of Homeland Security (“DHS”),¹ Kevin McAleenan (“McAleenan”), Acting Commissioner of U.S. Customs and Border Protection (“CBP”), and Thomas Homan (“Homan”), Acting Director of U.S. Immigration and Customs Enforcement (“ICE”) (collectively, “Defendants”). D. 7 ¶¶ 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 ¶¶ 1-10, 168-73. They seek declaratory and injunctive relief. D. 7 at 40-42. Defendants have now moved to dismiss. D. 14. For the reasons stated below, the Court DENIES Defendants’ motion to dismiss.

¹ The initial suit was filed against Elaine Duke, then Acting Secretary of DHS, but Nielsen has been substituted as Secretary of Homeland Security pursuant to Fed. R. Civ. P.25(d)

II. Standard of Review

To survive a motion to dismiss under Fed. R. Civ. P.12(b)(6), a complaint must include “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007); *García-Catalán v. United States*, 734 F.3d 100, 103 (1st Cir. 2013). The Court “must assume the truth of all well-plead[ed] facts and give the plaintiff the benefit of all reasonable inferences therefrom.” *Ruiz v. Bally Total Fitness Holding Corp.*, 496 F.3d 1, 5 (1st Cir. 2007). Plaintiffs “need not demonstrate that [they are] likely to prevail” at this stage, *García-Catalán*, 734 F.3d at 102, but they must show that the combined allegations state “a plausible, not a merely conceivable, case for relief.” *Sepúlveda-Villarini v. Dept of Educ. of P.R.*, 628 F.3d 25, 29 (1st Cir. 2010).

III. Factual Background

Unless otherwise noted, the following facts are drawn from Plaintiffs’ amended complaint and accepted as true for the purposes of considering the motion to dismiss. Plaintiffs are individuals whose electronic devices have been searched by federal officers at U.S. ports of entry on at least one occasion, and who “regularly travel outside the country with their electronic devices and intend to continue doing so.” D. 7 ¶ 2. Defendants are the heads of DHS and two of its units, CBP and ICE. D. 7 ¶ 3.

In the United States, ninety-five percent of adults own a cell phone, seventy-seven percent own a smart phone and over fifty percent own a tablet computer. D. 7 ¶ 27. “Electronic devices are often essential to people’s work,” as well as “communication . . . navigation, shopping, banking, entertainment,

news, and photography, among other functions.” D. 7 ¶¶ 36, 27. “Laptops sold in 2017 can store up to two terabytes” of data, tablet computers can hold up to a terabyte and “smartphones can store hundreds of gigabytes of data.” D. 7 ¶ 30. This storage capacity “can be the equivalent of hours of video files, thousands of pictures, or millions of pages of text.” *Id.* Electronic devices like these may also be used to access cloud storage—“data located on remote servers”—as well as email and social media applications. D. 7 ¶¶ 30, 32. Data stored on electronic devices includes “personal, expressive, and associational information” like communications, location history, contact lists, internet browsing history, photos, calendars and notes. D. 7 ¶ 31. Additionally, electronic devices store “historical location information, so-called ‘deleted’ items that actually remain in digital storage,” “metadata about digital files” and “time stamps or GPS coordinates created automatically by software on the device.” D. 7 ¶ 33.

According to public CBP data, “CBP conducted 14,993 electronic device searches in the first half of fiscal year 2017,” putting CBP “on track to conduct approximately 30,000 searches this fiscal year, compared to just 8,503 searches in fiscal year 2015.” D. 7 ¶ 38.² Searches generally come in two forms: (1)

² See *CBP Releases Statistics on Electronic Device Searches*, U.S. Customs and Border Protection (Apr. 11, 2017), <http://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0>. Indeed, according to CBP’s reported statistics postdating Plaintiffs’ amended complaint, CBP’s electronic device search rate remained consistent in the second half of fiscal year 2017, which ran until September 30, 2017, and the number of travelers whose

“manual” searches, during which “officers review the contents of the device by interacting with it as an ordinary user would, through its keyboard, mouse, or touchscreen interfaces”; and (2) “forensic” searches, during which officers “use sophisticated tools, such as software programs or specialized equipment, to evaluate information contained on a device,” typically starting by making a copy of the device’s data. D. 7 ¶¶ 39, 40, 43. Forensic searches “can capture all active files, deleted files, files in allocated and unallocated storage space, metadata . . . password-protected or encrypted data, and log-in credentials and keys for cloud accounts.” D. 7 ¶ 43. On occasion, officers confiscate travelers’ devices for prolonged periods. D. 7 ¶¶ 50-56.

CBP and ICE have policies that authorize and guide agents’ search of travelers’ electronic devices at border locations. D. 7 ¶¶ 8, 57-61. Both units’ policies permit searches of electronic devices without a showing of probable cause or issuance of a search warrant. D. 7 ¶¶ 9, 57.

A. The Search Policies

The CBP and ICE electronic device search policies detailed below are matters of public record, published by DHS and available to the public and, accordingly, may be considered by the Court for the purposes of this motion. *See Alt. Energy, Inc. v. St. Paul Fire & Marine Ins. Co.*, 267 F.3d 30, 33 (1st Cir.

electronic devices were searched totaled 30,200. D. 18-2 at 5 n.7; *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics*, U.S. Customs and Border Protection (Jan. 5, 2018), <http://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive>

2001). Moreover, neither party challenges that the Court may take judicial notice of these policies, but rather, request that the Court does so. *See* D. 18; D. 19 at 13 n.1. The Court, therefore, takes judicial notice of the following policies: ICE’s directive number 7-6.1, issued August 18, 2009, titled “Border Searches of Electronic Devices” (“ICE Policy”); CBP directive number 3340-049, issued August 20, 2009, titled “Border Searches of Electronic Devices Containing Information” (“2009 CBP Policy”);³ and CBP’s directive number 3340-049A, issued January 4, 2018, superseding the 2009 CBP Policy, titled “Border Search of Electronic Devices” (“2018 CBP Policy”), D. 18-1.

1. *The ICE Policy*

The ICE Policy establishes procedures “to search, detain, seize, retain, and share information contained in electronic devices possessed by individuals at the border” and “applies to . . . all persons arriving in, departing from, or transitioning through the United States.” ICE Pol. ¶ 1.1. It states that “[a]ll electronic devices crossing U.S. borders are subject to border search,” defining “electronic devices” 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.” ICE Pol. ¶¶ 8.6.1, 5.2.

³ As of this opinion’s publication, the 2009 ICE Policy is available at the following online address: https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf (“ICE Pol.”). The 2009 CBP Policy is available at https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf (“2009 CBP Pol.”).

Under the ICE Policy, agents are authorized to search electronic devices “with or without individualized suspicion.” D. 7 ¶ 58(b); ICE Pol. ¶ 6.1. “To the extent practicable, border searches should be conducted in the presence of, or with the knowledge of, the traveler.” ICE Pol. ¶ 8.1.2. The traveler’s consent, however, is not needed for search. ICE Pol. ¶ 8.1.3.

No individualized suspicion is required for officers to confiscate devices or “copies of information therefrom” for “further review” on- or off-site. ICE Pol. ¶¶ 6.1, 8.1.4; *see* D.7 ¶ 61(b). Additionally, “[a]ssistance to complete a border search may be sought from other Federal agencies and non-Federal entities, on a case by case basis, as appropriate,” for technical or subject matter assistance. ICE Pol. ¶¶ 6.1, 8.1.4, 8.4. ICE agents “may create and transmit copies of information” when seeking assistance. ICE Pol. ¶ 8.4.4. Such assistance “is to be accomplished within a reasonable period of time.” ICE Pol. ¶ 8.4.5.a. In general, once ICE confiscates a device, ICE may retain it for “a reasonable time given the facts and circumstances of the particular search,” generally thirty days, and supervisors may extend this period under “circumstances . . . that warrant more time.” ICE Pol. ¶ 8.3.1; D. 7 ¶ 61(c).

Regarding written records of searches, “[n]othing 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.” ICE Pol. ¶ 6.3. If ICE confiscates a device, agents must “provide the traveler with a copy of the applicable chain of custody form or other appropriate documentation.” ICE Pol. ¶ 8.2.4. ICE agents may seize and retain

devices or copies of information contained therein if they determine there is probable cause of unlawful activity or, to “the extent authorized by law,” information “relevant to immigration, customs, and other law enforcement matters.” ICE Pol. ¶¶ 8.5.1.a-b. Copies may be shared with federal, state, local and foreign law enforcement agencies. ICE Pol. ¶ 8.5.1.c.

The ICE Policy states that copies of information “determined to be of no relevance to ICE will be destroyed . . . within seven business days after conclusion of the border search unless circumstances require additional time” and “no later than 21 calendar days after conclusion of the border search.” ICE Pol. ¶ 8.5.1.e. Assisting agencies must return devices and data to ICE or “certify to ICE that any copies in its possession have been destroyed” unless they have the independent legal authority to retain copies. ICE Pol. ¶ 8.5.2. Non-federal entities must return all copies of information “as expeditiously as possible.” ICE Pol. ¶ 8.5.3.

2. *The CBP Policies*

Given that Plaintiffs seek injunctive, prospective relief, the Court relies primarily upon the 2018 CBP Policy, as it supersedes the 2009 CBP Policy. *See* D. 18-1 at 2. For the purposes of any relief sought to address past harms, however, the Court briefly outlines the 2009 CBP Policy below to the extent it differs from the 2018 CBP Policy.

a) The 2018 CBP Policy

The 2018 CBP Policy applies to searches performed by CBP officers, not ICE or Homeland Security Investigations (“HSI”) agents. D. 18-1 ¶ 2.7. It defines “electronic device” as “[a]ny device that may

contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players.” D. 18-1 ¶ 3.2.

The 2018 CBP Policy divides electronic device searches into two categories: the basic search and the advanced search. D. 18-1 ¶ 5.1. An “advanced search” is defined as “any search in which an Officer connects external equipment . . . to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents.” D. 18-1 ¶ 5.1.4. It requires “reasonable suspicion of activity in violation of the laws enforced or administered by CBP” or a “national security concern,” as well as “supervisory approval,” to justify the search. *Id.* A supervisor must also be present during the search. D. 18-1 ¶ 5.1.5. A “basic search,” by contrast, is “[a]ny border search of an electronic device that is not an advanced search.” D. 18-1 ¶ 5.1.3. An officer may conduct such a search “with or without suspicion.” *Id.*

All electronic device searches are documented. D. 18-1 ¶ 5.1.5. Additionally, all searches “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.” D. 18-1 ¶ 5.1.6. Permission to remain present, however, “does not necessarily mean that the individual shall observe the search itself.” *Id.*

The 2018 CBP Policy authorizes “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.” D.

18-1 ¶ 5.1.2. The policy prohibits an officer's intentional search of information stored remotely, directing officers to request that travelers "disable connectivity to any network" prior to search. *Id.* According to the policy, "[t]ravelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents," and "[p]asscodes or other means of access may be requested and retained as needed to facilitate" the search. D. 18-1 ¶ 5.3.1. If an officer cannot complete an inspection because of passcode or encryption protection, the officer may "detain the device pending a determination as to its admissibility, exclusion, or other disposition" or "seek technical assistance" or "use external equipment" to access the device. D. 18-1 ¶¶ 5.3.3-4.

The 2018 CBP Policy permits officers to "detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time," which "ordinarily should not exceed five (5) days," on- or off-site, but may be extended with supervisor approval. D. 18-1 ¶ 5.4.1. If a device is detained, the officer must issue a custody receipt to the traveler prior to the traveler's departure, D. 18-1 ¶ 5.4.1.4, and all transfers of custody must be recorded, D. 18-1 ¶¶ 5.4.2.3, 5.6.2. CBP officers may make copies of electronic devices when seeking technical assistance—e.g., device access or translation assistance—or subject matter assistance "with reasonable suspicion or national security concern." D. 18-1 ¶¶ 5.4.2.1-2. Unless assistance is sought within CBP or from ICE, requests for assistance require supervisory approval and must be documented. D. 18-1 ¶ 5.4.2.3.

If after a review of the electronic device an officer determines there is probable cause to believe it contains evidence of illegal activity, officers “may seize and retain” the device. D. 18-1 ¶ 5.5.1.1. “Without probable cause . . . 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.” D. 18-1 ¶ 5.5.1.2. The 2018 CBP Policy does not limit CBP’s authority to share information from these devices, “retained in accordance with this Directive, with federal, state, local, and foreign law enforcement agencies.” D. 18-1 ¶ 5.5.1.3.

If the review does not give rise to “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” within seven days of such determination, barring special circumstances. D. 18-1 ¶ 5.4.1.2. Additionally, “[p]asscodes and other means of access obtained during the course of a border inspection . . . will be deleted or destroyed when no longer needed to facilitate the search.” D. 18-1 ¶ 5.3.2. To the extent any assistance was provided outside of CBP or ICE, the assisting agency or entity “should destroy all copies of the information conveyed.” D. 18-1 ¶ 5.5.2.2. “The destruction shall be noted in appropriate CBP systems.” D. 18-1 ¶ 5.4.1.2.

b) The 2009 CBP Policy

Under the 2009 CBP Policy, which was in force at the time of Plaintiffs’ alleged border device searches, certain policies differed. The 2009 CBP Policy did not distinguish between a basic and advanced search and no level of suspicion was

required for either. D. 7 ¶ 61(a); 2009 CBP Pol. ¶ 5.1.2. Likewise, the earlier policy permitted confiscation of electronic devices for on- or off-site search without any level of suspicion. D. 7 ¶ 61(a); 2009 CBP Pol. ¶ 5.3.1.

B. The Plaintiffs

1. *The Alasaads*

Ghassan and Nadia Alasaad are U.S. citizens and Massachusetts residents whose two smartphones were searched and retained when they were crossing the border in July 2017 from Canada to Vermont. D. 7 ¶¶ 14, 62, 70. They were traveling with their eleven-year-old daughter, who was “ill and had a high fever.” D. 7 ¶ 63. When asked, a CBP supervisor told them they were being detained and searched because he “simply felt like ordering a secondary inspection.” D. 7 ¶ 66. In a secondary inspection room, a CBP officer manually searched Ghassan’s smartphone. D. 7 ¶ 65. Several hours later, a CBP officer ordered Nadia to provide the password to her locked phone. D. 7 ¶ 67. After the officer told them that if Nadia did not disclose her password, the “phone would be confiscated,” she wrote down the password. D. 7 ¶ 68. Nadia “wears a headscarf in public in accordance with her religious beliefs” and told the officer that a male officer could not search her phone because it contained photos of her without a headscarf and the officer responded “that it would take two hours for a female officer to arrive, and then more time to search the phone.” D. 7 ¶¶ 67, 70. After approximately six hours of detention, the Alasaads departed without their two phones. D. 7 ¶¶ 70-71. The phones were returned fifteen days later. D. 7 ¶ 72. CBP’s search and seizure of Ghassan’s phone “damaged its functionality.” *Id.*

One month later, the Alasaads' daughter's locked smartphone was searched when Nadia and her daughter arrived in New York from Morocco "where they had been visiting family." D. 7 ¶¶ 73, 75. CBP officers directed the two to a secondary inspection area. D. 7 ¶ 74. There, Nadia informed the officers that she had lost her phone, but when officers searched Nadia's purse, they found her daughter's smartphone. *Id.* The officers directed the Alasaads' daughter to write down her password, and after she did, an officer "took the phone to another room for approximately 15 minutes." D. 7 ¶ 75.

2. *Allababidi*

In January 2017, Allababidi had his devices searched and confiscated by CBP officers when returning from a business trip on a flight from Dubai to Dallas. D. 7 ¶¶ 77-80. A U.S. citizen who lives in Texas and owns and operates a business that sells security technology, Allababidi carried a locked smartphone "that he used regularly for both personal and business matters" in the U.S. and an unlocked smartphone that "enabled him to communicate easily while overseas." D. 7 ¶¶ 15, 77. A CBP officer directed Allababidi to a secondary inspection area, where he observed an officer "seize and manually search his unlocked phone for at least 20 minutes." D. 7 ¶ 78. The officer ordered Allababidi to unlock his other phone, and when he declined, officers confiscated both smartphones. D. 7 ¶ 79. One phone was returned two months later, and the other had not been returned at the time the amended complaint was filed. D. 7 ¶ 80.

3. *Bikkannavar*

Bikkannavar, a U.S. citizen residing in California, returned from a vacation in Chile with a locked smartphone owned by his employer, NASA's Jet Propulsion Laboratory, which he used for work and personal matters. D. 7 ¶¶ 16, 81. CBP officers escorted Bikkannavar to a secondary inspection area, where an officer gave him a CBP form that Bikkannavar understood to "mean that CBP was asserting a legal prerogative to search the contents of his phone." D. 7 ¶ 82. After initially declining to do so, Bikkannavar disclosed his password, which an officer wrote down and took, with Bikkannavar's phone, to another room. D. 7 ¶¶ 82-83. The officer returned about thirty minutes later, informed Bikkannavar that officers had used "algorithms" to search its contents, and returned the phone. D. 7 ¶ 84.

4. *Dupin*

Dupin, a journalist, citizen of Haiti and legal permanent resident of the U.S. living in Massachusetts, was subject to two device searches in December 2016. D. 7 ¶¶ 17, 86-97. In the first, Dupin connected in Miami, Florida, en route from Port-au-Prince, Haiti to Montreal, Quebec, where he was visiting his daughter to take her by bus to New York City. D. 7 ¶ 86. A CBP officer escorted Dupin to a secondary inspection area in Miami, where he waited for over two hours before being escorted to a smaller room for questioning "about his work as a journalist, including the names of the organizations and specific individuals within those organizations for whom he had worked" by three CBP officers. D. 7 ¶ 87. During questioning, officers seized Dupin's locked smartphone and ordered him to provide a password,

which he did. D. 7 ¶ 88. An officer searched Dupin’s phone for “about two hours” during which, at certain points, the officer took Dupin’s phone “into another room,” returning “periodically to ask Mr. Dupin questions about the contents of the phone.” D. 7 ¶ 90. The officers then returned the phone and permitted him to leave. D. 7 ¶ 91.

The next day, December 23, 2016, Dupin and his seven-year-old daughter traveled by bus from Montreal to New York. D. 7 ¶ 92. At the customs checkpoint “near midnight,” a CBP officer directed them to a secondary inspection area, where officers asked “some of the same questions officers had asked in Miami” as his daughter was “[a]sleep in his lap.” D. 7 ¶¶ 93, 95(d). The officers seized his phone, obtained his password, and took the “phone into another room for about four hours,” again returning periodically with specific questions about the phone’s contents. D. 7 ¶¶ 94, 96. “After approximately seven hours of detention,” on the morning of December 24, 2016, officers returned the phone to Dupin and told him that he and his daughter could leave. D. 7 ¶ 97.

5. *Gach*

Gach, an artist and U.S. citizen who lives in California, had his locked smartphone searched on arrival in San Francisco from Belgium, “where he had participated in an art exhibition displaying works that could be considered critical of the government.” D. 7 ¶ 18, 98-104. He was questioned “about his work as an artist and the exhibition in Belgium” in a secondary inspection area, and, when asked for his phone, told the officers that he did not want the officers to search it. D. 7 ¶ 99. After “[t]he officers told [him]that his phone would be held for an indeterminate amount of

time if he did not disclose his password,” Gach entered his password and handed the officers his unlocked phone. D. 7 ¶ 100. The officers searched Gach’s phone “behind a dividing wall for approximately 10 minutes” and then returned the phone to him and permitted him to leave. D. 7 ¶¶ 102-04.

6. *Kushkush*

Kushkush—a U.S. citizen and freelance journalist from Virginia—had his devices searched on three occasions between January 2016 and July 2017. D. 7 ¶¶ 19, 105-19. First, in New York, Kushkush, while returning from conducting research for a master’s thesis in Stockholm, Sweden, was questioned by CBP officers, who also seized his locked laptop and two unlocked cell phones. D. 7 ¶¶ 105-07. They searched the devices out of his sight for around twenty minutes before returning them to him. D. 7 ¶ 107.

In January 2017, Kushkush flew to Washington, D.C. from Israel, where he had completed an internship with the Associated Press, carrying a “locked smartphone that he used for both professional and personal matters,” the same locked laptop and unlocked devices including a digital camera, voice recorder and flash drives. D. 7 ¶ 108. In a secondary inspection area, CBP officers questioned him “about his reporting activities,” asked for his social media identifiers and email address, and instructed Kushkush to unlock his phone. D. 7 ¶¶ 109-10. Kushkush “reluctantly complied” and observed the officer manually search the phone. D. 7 ¶¶ 110-12. Officers took the other devices “into another room for approximately 20 minutes.” D. 7 ¶ 112. The officers returned the devices and he was permitted to leave. D. 7 ¶ 113.

In July 2017, Kushkush returned to the U.S. on a bus from Montreal with fellow students in a language program, and at the border, he was directed to secondary inspection. D. 7 ¶¶ 114-15. Kushkush unlocked his phone for the CBP officer, “stat[ing] that he was doing so against his will,” and the officer wrote down Kushkush’s password and took the phone out of Kushkush’s sight “for at least one hour.” D. 7 ¶¶ 115-17. Officers also questioned Kushkush “about his work as a journalist.” D. 7 ¶ 118. After “approximately three and a half hours,” CBP officers returned the phone and permitted Kushkush to leave. D. 7 ¶ 119.

7. *Maye*

Maye, a U.S. citizen from Florida, assistant professor of homeland security at Embry-Riddle Aeronautical University and former U.S. Air Force captain, flew from vacation in Oslo, Norway, to Miami with a locked laptop and smartphone. D. 7 ¶¶ 20, 120. In a secondary inspection area with two CBP officers, Maye unlocked her devices after being ordered to do so. D. 7 ¶¶ 121-22. Maye observed an officer manually search her unlocked laptop. D. 7 ¶ 123. An officer also “seized” her “unlocked phone for approximately two hours.” D. 7 ¶ 124.

8. *Merchant*

Merchant is a U.S. citizen, founder and editor of a media organization that publishes online news content and a graduate student in international security and journalism at Harvard University. D. 7 ¶¶ 21, 125. In March 2017, after visiting her uncle in Toronto, Ontario, Merchant was directed to a secondary inspection area at a U.S. customs preclearance station in the Toronto airport prior to her

flight home to Orlando. D. 7 ¶¶ 126-27. After CBP officers asked for Merchant’s smartphone, Merchant—who “wears a headscarf in public in accordance with her religious beliefs” and whose phone contains photos of her without her headscarf—told CBP officers she would give them the phone but not unlock it. D. 7 ¶ 129. CBP officers repeatedly told her she “could choose to unlock the phone, or have it seized indefinitely.” D. 7 ¶ 129-30. Merchant told the officers she was traveling alone and needed the phone to communicate and for her work. D. 7 ¶ 130. “In tears, Ms. Merchant unlocked her phone” and “provided the password to unlock her laptop.” D. 7 ¶ 131. CBP officers searched Merchant’s laptop and phone out of her sight for approximately one and a half hours. D. 7 ¶ 135. Officers questioned her about her religious affiliation and certain of her blog posts. D. 7 ¶ 133. “When the CBP officers returned the phone to Ms. Merchant and she unlocked it, the Facebook application was open to the ‘friends’ page. It had not been open to that page when she had given up the phone.” D. 7 ¶ 135.

9. *Shibly*

Shibly, a U.S. citizen and filmmaker from Buffalo, New York, had his devices searched on two occasions in January 2017. D. 7 ¶¶ 22, 136-46. First, returning home by car from Canada, Shibly was directed to a secondary inspection area at the border in New York, and told to “fill out a form with information that included . . . his phone’s password.” D. 7 ¶¶ 136-37. An officer then “ordered” him to provide the password, saying that “if he had nothing to hide, then he should unlock his phone,” and Shibly “disengaged” the lock on the phone. D. 7 ¶¶ 137-38.

Shibly also provided CBP officers with his social media identifiers. D. 7 ¶ 141. Shibly’s phone was taken out of his sight for an hour before it was returned and he was permitted to leave. D. 7 ¶¶ 140, 142. Three days later, Shibly was stopped on the same bridge and directed to a secondary inspection area. D. 7 ¶¶ 143-44. When he declined to hand over his phone, “[t]hree CBP officers . . . used physical force to seize his phone.” D. 7 ¶ 145. An officer took the phone—which was still unlocked from the first search—to a different room. D. 7 ¶¶ 143, 146.

10. Wright

Wright, a computer programmer from Colorado, was brought to an inspection area in the Denver airport after returning home from a trip in Southeast Asia. D. 7 ¶¶ 23, 147-48. A CBP officer ordered Wright to unlock his laptop and when Wright declined, CBP officers confiscated the laptop as well as his locked phone and his camera. D. 7 ¶ 148. According to CBP documents disclosed to Wright in a Freedom of Information Act and Privacy Act (“FOIA”) request, CBP confiscated Wright’s devices pursuant to instructions from ICE’s Homeland Security Investigations (“HSI”) division, which sought “further forensic review.” D. 7 ¶ 149. These records demonstrate that HSI “attempted to image” Wright’s laptop and a CBP forensic scientist extracted data from Wright’s phone and camera, which he stored on three thumb drives he sent to other CBP officers. D. 7 ¶ 152. Wright received his devices fifty-six days later. D. 7 ¶ 154. CBP documentation from Wright’s FOIA request does not reflect destruction of the information extracted from Wright’s devices. D. 7 ¶ 155c.

IV. Procedural History

Plaintiffs instituted this action on September 13, 2017. D. 1; D. 7. Defendants now move to dismiss. D. 14. On April 23, 2018, the Court heard the parties on the pending motion and took the matter under advisement. D. 33.

V. Discussion

Defendants argue that Plaintiffs do not have standing to bring this suit, and that even if they do, they have failed to state a claim on the merits. D. 14. The Court addresses standing as a threshold inquiry because “[i]f a party lacks standing to bring a matter before the court, the court lacks jurisdiction to decide the merits of the underlying case.” *United States v. AVX Corp.*, 962 F.2d 108, 113 (1st Cir. 1992).

A. Standing

“Standing to sue is a doctrine rooted in the traditional understanding of a case or controversy” within Article III of the U.S. Constitution, *Spokeo, Inc. v. Robins*, ___ U.S. ___, 136 S. Ct. 1540, 1547 (2016), and serves to “identify those disputes which are appropriately resolved through the judicial process,” *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990). “The law of Article III standing, which is built on separation of powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 408 (2013). 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*, 136 S. Ct. at 1547; *see Lujan v. Defs.*

of *Wildlife*, 504 U.S. 555, 560-61 (1992). Plaintiffs bear the burden of establishing standing, but “the same pleading standards apply both to standing determinations and Rule 12(b)(6) determinations.” *Hochendoner v. Genzyme Corp.*, 823 F.3d 724, 734 (1st Cir. 2016); see *Lujan*, 504 U.S. at 561; *Reddy v. Foster*, 845 F.3d 493, 497 (1st Cir. 2017).

“The ‘[f]irst and foremost’ concern in standing analysis is the requirement that the plaintiff establish an injury in fact” *Reddy*, 845 F.3d at 500 (quoting *Spokeo*, 136 S. Ct. at 1547) (alteration in original). To do so, “a plaintiff must show that he or she suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Spokeo*, 136 S. Ct. at 1548 (quoting *Lujan*, 504 U.S. at 560). “[T]he imminence concept, while admittedly far reaching, is bounded by its Article III purpose: ‘to ensure that the alleged injury is not too speculative.’” *Berner v. Delahanty*, 129 F.3d 20, 24 (1st Cir. 1997) (quoting *Lujan*, 504 U.S. at 564 n.2). Where, as here, Plaintiffs seek injunctive relief, they must plausibly allege that “the threatened injury is ‘certainly impending’ or there is a ‘substantial risk that the harm will occur.’” *Susan B. Anthony List v. Driehaus* (“*SBA List*”), ___ U.S. ___, 134 S. Ct. 2334, 2341 (2014) (quoting *Clapper*, 568 U.S. at 414, 414 n.5); see *Reddy*, 845 F.3d at 500. Because we are “[a]t the pleading stage, general factual allegations of injury resulting from the defendant[s]’ conduct may suffice.” *Lujan*, 504 U.S. at 561; see *Hochendoner*, 823 F.3d at 731.

“[S]tanding is not dispensed in gross” *Lewis v. Casey*, 518 U.S. 343, 358 n.6 (1996). Rather, the standing inquiry is a “plaintiff-by-plaintiff and claim-

by-claim analysis.” *Hochendoner*, 823 F.3d at 733. The Court must, therefore, determine “whether each particular plaintiff is entitled to have a federal court adjudicate each particular claim that he asserts.” *Id.* (quoting *Pagán v. Calderón*, 448 F.3d 16, 26 (1st Cir. 2006)). Defendants argue that Plaintiffs do not have standing to seek declaratory or injunctive relief for any alleged Fourth or First Amendment violations and that they also lack standing to seek expungement.⁴ D. 15 at 15-22. The Court addresses each claim in turn.

1. *Standing to Seek Injunctive or Declaratory Relief*

Plaintiffs allege that they “face a likelihood of future injury caused by the challenged policies and practices . . . related to searching and seizing electronic devices at the border.” D. 7 ¶ 156. Although each Plaintiff has individual reasons for doing so, “[a]ll Plaintiffs have traveled across the U.S. border with their electronic devices multiple times” and “will continue to do so in the future.” *Id.* At the border, “they will be subject to CBP’s and ICE’s policies and practices . . . namely, search or seizure of their devices absent a warrant, probable cause or reasonable suspicion,” and Plaintiffs cannot avoid this harm without “forego[ing] international travel or [] travel[ing] without any electronic devices, which would cause great hardship.” *Id.* On this basis,

⁴ Defendants also argue that allegations of potentially chilled speech fail to establish standing, D. 15 at 21-22, but Plaintiffs respond that they do not rely upon “the chill of their First Amendment rights” as they alleged injury to support standing here, D. 19 at 16 n.3. The Court will not, therefore, address that theory further.

Plaintiffs seek to enjoin Defendants from “searching electronic devices absent a warrant supported by probable cause that the devices contain” evidence of illegal activity and from “confiscating travelers’ electronic devices, to effectuate searches of those devices after travelers leave the border, absent probable cause.” D. 7 at 41-42.

Defendants argue that Plaintiffs’ allegations fail to allege plausibly any “certainly impending” injury, *Clapper*, 568 U.S. at 414. D. 15 at 17. As the First Circuit explained recently, however, the Supreme Court in *SBA List*—which “both postdated and cited *Clapper*”—established a “disjunctive framing of the test: injury is imminent if it is certainly impending *or* if there is a substantial risk that harm will occur.” *Reddy*, 845 F.3d at 500 (emphasis in original). Thus, even if Plaintiffs do not allege an injury that is “certainly impending,” they may still establish standing by plausibly alleging a substantial risk that harm will occur. *See id.*; *SBA List*, 134 S. Ct. at 2341.

Defendants contend that Plaintiffs have also failed to satisfy the “substantial risk” inquiry. D. 15 at 17-19. Plaintiffs allege that CBP data demonstrates that it is on track to conduct approximately 30,000 searches this fiscal year. D. 7 ¶ 38. Defendants point out, however, that those searches only amounted to 0.008% of the approximately 189.6 million travelers who arrived at U.S. borders during this period. D. 15 at 17-18. Defendants argue that this future search probability—which they characterize as a “slight chance” of search—is not sufficient to establish standing here. D. 15 at 18.

There is no numerical threshold, however, at which likelihood of harm becomes a “substantial risk”

of harm. See *Kerin v. Titeflex Corp.*, 770 F.3d 978, 983 (1st Cir. 2014) (noting that “a small probability of a great harm may be sufficient”). Although 0.008% may be a small percentage of total travelers, the searches still occur at an average of approximately 2500 searches per month. D. 7 ¶ 38. In *SBA List*, the Supreme Court supported its conclusion that there was a substantial likelihood of future harm with the explanation that proceedings enforcing the statute in question were “not a rare occurrence,” with twenty to eighty such cases occurring per year. *SBA List*, 134 S. Ct. at 2345. Against this backdrop, 30,000 searches per year is not a “rare occurrence,” even if it makes up a small percentage of total travelers. Moreover, “[e]ven a small probability of injury is sufficient to create a case or controversy—to take a suit out of the category of hypothetical—provided of course that the relief sought would, if granted, reduce the probability.” *Massachusetts v. EPA*, 549 U.S. 497, 525 n.23 (2007) (quoting *Village of Elk Grove Village v. Evans*, 997 F.2d 328, 329 (7th Cir. 1993)); see *NRDC v. EPA*, 464 F.3d 1, 7 (D.C. Cir. 2006) (holding 1 in 200,000 odds of developing skin cancer sufficient to support standing). Additionally, as the Court explains below, that four Plaintiffs here have been subjected to multiple searches, D. 7 ¶¶ 62-76, 86-97, 105-19, 136-46, suggests that the risk of future search is higher for these plaintiffs than the general population.

Defendants also argue that Plaintiffs’ allegations of future harm are impermissibly “vague” and speculative. D. 15 at 17-18. They point to Reddy for the proposition that in the First Circuit, “[s]peculation’ that a government actor ‘might in the future take some other and additional action

detrimental to' Plaintiffs, is 'not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm.'" D. 15 at 18 (quoting *Reddy*, 845 F.3d at 503). In *Reddy*, however, the First Circuit held that the plaintiffs' assertions of standing were speculative as to a New Hampshire buffer zone statute, emphasizing that the statute had not yet been enforced. *Reddy*, 845 F.3d at 496, 503. Here, by contrast, Plaintiffs challenge policies that are in place and are being actively enforced. D. 7 ¶¶ 37-38; see *SBA List*, 134 S. Ct. at 2346 (finding standing to enjoin enforcement of state statute that had been enforced for decades); *Dudley v. Hannaford Bros. Co.*, 333 F.3d 299, 306 (1st Cir. 2003) (explaining that a "real and immediate threat" of injury may be demonstrated through an "offending policy [that] remains firmly in place"). Plaintiffs' alleged future injury does not depend upon defendants' future illegal conduct untethered to a pattern of past practice, cf. *Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983) (concluding that plaintiff subject to illegal arrest procedure made no showing that he was likely to be arrested and subjected to illegal procedure again), but rather upon recurring conduct authorized by official policies.

That is, Plaintiffs' subjection to prior searches further bolsters their allegations of likely future searches. Although "[p]ast exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief," *Lujan*, 504 U.S. at 564 (quoting *Lyons*, 461 U.S. at 102), "[p]ast wrongs [a]re evidence bearing on 'whether there is a real and immediate threat of repeated injury,'" *Lyons*, 461 U.S. at 102 (quoting *O'Shea v. Littleton*, 414 U.S. 488, 496

(1974)). See, e.g., *Morales v. Chadbourne*, 996 F. Supp. 2d 19, 37-38 (D.R.I. 2014) (finding standing for American citizen who had been inappropriately detained by ICE twice and warned that it could happen again); *Thomas v. Cty. of L.A.*, 978 F.2d 504, 507 (9th Cir. 1992) (explaining that the “possibility of recurring injury ceases to be speculative when actual repeated incidents are documented” (quoting *Nicacio v. U.S. INS*, 797 F.2d 700, 702 (9th Cir. 1985))); cf. *Penobscot Nation v. Mills*, 861 F.3d 324, 336-37 (1st Cir. 2017) (denying standing at summary judgment where there was no evidence of prior enforcement of the policy in question against the plaintiffs). Here, all Plaintiffs have been subjected to electronics searches at the border and four Plaintiffs have been subjected to multiple device searches. D. 7 ¶¶ 2, 62-155. Plaintiffs’ theory of standing, therefore, is sufficiently concrete to plausibly allege injury-in-fact.

Plaintiffs’ allegations of future harm are no less concrete because they omit specific plans or dates of future travel. Defendants argue that without such details, Plaintiffs have merely expressed “some day” intentions to travel, which are not enough to establish actual or imminent injury. D. 15 at 19 (quoting *Lujan*, 504 U.S. at 564). In *Lujan*, the two individuals in question stated in affidavits that they intended to return to the habitats in question sometime “in the future,” which was insufficient to establish “at the summary judgment stage, a factual showing of perceptible harm.” *Lujan*, 504 U.S. at 563-64, 566. As a result, with plaintiffs “alleg[ing] only an injury at some indefinite future time,” the Court held that the “imminence” requirement for future injury had “been stretched beyond the breaking point.” *Id.* at 564 n.2.

As Justice Kennedy explained in his concurring opinion, the requirement for travel specifics was warranted in that case because it was “not a case where it [wa]s reasonable to assume that the affiants will be using the sites on a regular basis . . . nor d[id] the affiants claim to have visited the sites since the projects commenced.” *Id.* at 579 (Kennedy, J., concurring) (citation omitted). Plaintiffs argue that their allegations sufficiently demonstrate a “realistic risk of future exposure to [the] challenged policy,” *Berner*, 129 F.3d at 24, through their allegations that they regularly travel outside the U.S. for work, visiting friends and family, vacation and tourism, D. 19 at 19-20; e.g., D. 7 ¶¶ 2, 62, 73, 77, 81, 86, 105, 114, 126, 143, and will continue to do so in the future, D. 7 ¶ 156.

This case is distinct from *Lujan* on several bases. First, this case is only at the motion to dismiss phase, unlike the summary judgment stage in *Lujan*, 504 U.S. at 561, 566. Second, exposure to CBP and ICE policy does not require travel to a specific destination, but rather only requires some international travel and return to the U.S.; it is reasonable to infer from the allegations in the complaint that these Plaintiffs will engage in international travel again in the future, *cf. id.* at 579 (Kennedy, J., concurring), particularly as Plaintiffs allege prior travel abroad and professional backgrounds that might warrant future travel. *See Lyons*, 461 U.S. at 102 (looking to plaintiffs’ prior actions to determine likelihood of future injury); *Lujan*, 504 U.S. at 592 (Blackmun, J., dissenting). Given this case’s posture, the breadth of activity that would compel exposure to the policies at issue and Plaintiffs’ allegations of prior travel and professional

activity, Plaintiffs' allegations in this context are sufficient to allege actual or imminent injury.

Finally, Defendants argue that Plaintiffs have failed to establish standing because their risk of injury is no greater than that of the general public, rendering their alleged harm a generalized grievance inappropriate for adjudication. D. 15 at 19. “[A] plaintiff raising only a generally available grievance about government—claiming only harm to his and every citizen’s interest in proper application of the Constitution and laws, and seeking relief that no more directly and tangibly benefits him than it does the public at large—does not state an Article III case or controversy.” *Lujan*, 504 U.S. at 573-74. Defendants focus solely upon whether Plaintiffs’ “future risk of a device search” is greater than that of the general public, D. 15 at 19, but simply that a harm may be “widely shared” does not eliminate a plaintiff’s standing to sue. *Massachusetts*, 549 U.S. at 522. Rather, plaintiffs lack standing under the generalized grievance rule when the alleged injury is “not only widely shared, but is also of an abstract and indefinite nature.” *FEC v. Akins*, 524 U.S. 11, 23 (1998). Plaintiffs may plausibly allege standing regardless of “how many persons have been injured by the challenged action” if they plausibly allege that their individual rights have been or will be infringed in some “concrete and personal way.” *Massachusetts*, 549 U.S. at 517, (quoting *Lujan*, 504 U.S. at 581 (Kennedy, J., concurring)); see *Akins*, 524 U.S. at 24; *Public Citizen v. U.S. Dep’t of Justice*, 491 U.S. 440, 449-50 (1989) (explaining that “[t]he fact that other citizens or groups of citizens might make the same complaint . . . does not lessen appellants’ asserted injury”). As

the Court has explained, Plaintiffs have plausibly alleged a concrete, personal injury in the form of violation of their individual rights.

Plaintiffs also argue that their risk of search is higher than that of the general public because they have been searched before. D. 19 at 20-21. This argument is supported by the multiple searches of four Plaintiffs, despite the aforementioned low probability of subjection of the general public to a border search. Plaintiffs argue that Defendants' policies "alert officers to the past searches and confiscations, which may increase the likelihood of repeated searches." D. 19 at 20 (citing *Tabbaa v. Chertoff*, No. 05-cv-582S, 2005 U.S. Dist. LEXIS 38189, 2005 WL 3531828, at *9 (W.D.N.Y. Dec. 22, 2005), *aff'd*, 509 F.3d 89 (2d Cir. 2007)), a contention that may be borne out by discovery.

For all of these reasons, the Court DENIES Defendants' motion to dismiss on the basis that Plaintiffs lack standing, as Plaintiffs have plausibly alleged that they face a substantial risk of future harm from Defendants' ongoing enforcement of their border electronics search policies.

2. *Standing to Seek Expungement*

Plaintiffs also seek expungement of all data or 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 42. Retention of data illegally obtained by law enforcement may constitute continued harm sufficient to establish standing to seek expungement. *See Tabbaa*, 509 F.3d at 96 n.2 (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). Defendants challenge Plaintiffs’ standing to seek expungement here. D. 15 at 20-21.

Defendants argue that, as a factual matter, standing to seek expungement has only been alleged as to one Plaintiff, Wright, whose information was allegedly extracted and not destroyed by CBP, as demonstrated through documents he obtained through a FOIA request. D. 15 at 20. Although Defendants correctly point out that “[n]either conclusory assertions nor unfounded speculation can supply the necessary heft” to establish standing, D. 15 at 20 (quoting *Hochendoner*, 823 F.3d at 731), Plaintiffs need not produce FOIA documentation to allege plausibly that information contained on their devices has been retained by CBP or ICE, especially given—as explained above—that this is the motion to dismiss stage of litigation.⁵ Three other Plaintiffs—

⁵ Defendants’ argument that the amended complaint only alleges that “CBP retained the information it extracted from Mr. Wright’s devices,” D. 7 ¶ 155, omitting any allegations of the same for other Plaintiffs, ignores other allegations in the pleading. D. 32 at 4 n.2. Plaintiffs explicitly allege that “[o]n information and belief, Plaintiffs are suffering the ongoing harm of CBP and ICE retaining (a) content copied from their devices or records reflecting content observed during searches of their devices, (b) content copied from their cloud-based accounts accessed through their devices or records reflecting” such content, “(c) their social media identifiers, and/or (d) their device passwords.” D. 7 ¶ 157. Plaintiffs have not, therefore, failed to

the Alasaads and Allababidi—also allege searches involving retention of their electronic devices for at least two weeks. D. 7 ¶¶ 70-72, 79-80. Six of the remaining seven Plaintiffs allege that during their “basic” or manual device searches, their devices were searched outside of their presence for a period of time between ten minutes and four hours.⁶ D. 7 ¶¶ 84, 90, 96, 102, 107, 112, 117, 135, 140, 146. Given that both ICE and CBP policies in place at the time authorized conducting advanced searches of electronic devices without any individualized suspicion, D. 7 ¶ 58, it is plausible to infer from these facts that advanced searches may have occurred during this time, *see* D. 7 ¶ 84 (alleging that agents stated they used “algorithms” to search Bikkannavar’s phone outside of his presence). These policies, including the 2018 CBP Policy, also sanction creating copies of data contained on the devices during—or to be used for—advanced searches, ICE Pol. ¶ 8.1.4; D. 18-1 ¶¶ 5.1.4, 5.4.1, or to retain the assistance of other agencies and third parties, ICE Pol. ¶ 8.4.4; D. 18-1 ¶¶ 5.4.2.1-2. It is plausible, therefore, to infer that data or information from the devices may have been copied or otherwise documented during these searches.

Defendants also argue that Plaintiffs do not have standing to seek expungement because expungement would not redress Plaintiffs’ alleged injury. D. 15 at 20-21. Redressability, the third standing requirement, *see Spokeo*, 136 S. Ct. at 1547, requires that Plaintiffs

allege that information was retained by Defendants.

⁶ Maye alleges that an officer “seized” her unlocked phone “for approximately two hours,” but the complaint does not allege that such seizure removed her phone from her presence. *See* D. 7 ¶ 124.

demonstrate “a likelihood that prevailing in the action will afford some redress for the injury.” *City of Bangor v. Citizens Commc’ns Co.*, 532 F.3d 70, 92 (1st Cir. 2008) (quoting *Me. People’s All. V. Mallinckrodt, Inc.*, 471 F.3d 277, 283 (1st Cir. 2006)). Plaintiffs’ burden to demonstrate redressability, as with injury, is “relatively modest” at the motion to dismiss stage. *Bennett v. Spear*, 520 U.S. 154, 171 (1997). Plaintiffs’ injury “is redressable if the relief sought can compensate the plaintiff for his losses or ‘eliminate any effects’ caused by a defendant’s challenged conduct.” *Janfeshan v. U.S. Customs & Border Prot.*, No. 16-cv-6915, 2017 U.S. Dist. LEXIS 151058, 2017 WL 3972461, at *6 (E.D.N.Y. Aug. 21, 2017) (quoting *Steel Co. v. Citizens for a Better Env’t*, 523 U.S. 83, 106 (1998)).

Plaintiffs have plausibly demonstrated that expungement of their data would afford some redress for their alleged injury here. Plaintiffs argue that retention of their information “compounds the violations of [their] Fourth Amendment rights, because Defendants remain free to use and exploit it or share it with other agencies that may do the same.” D. 19 at 24; *see Tabbaa*, 509 F.3d at 96 n.2; *Hedgepath*, 386 F.3d at 1152. Defendants argue that expungement “would not likely result from a favorable resolution of [Plaintiffs’] claims” because “[t]he government’s use of ‘evidence obtained in violation of the Fourth Amendment does not itself violate the Constitution.” D. 15 at 20 (quoting *Pa. Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 362 (1998)). First, however, Defendants’ argument does not go to redressability, but rather to the merits of the constitutional claim and remedy sought. Defendants

do not argue that expungement would insufficiently redress Plaintiffs’ alleged injury—continued violation of the Fourth Amendment through retention of Plaintiffs’ data—but rather suggest that retention of Plaintiffs’ data is not itself a violation of the Fourth Amendment. D. 15 at 20-21. Indeed, to the extent Plaintiffs’ information was copied or obtained, subsequently retained and not destroyed by CBP or ICE, the destruction of these copies or data could redress such injury. *See Janfeshan*, 2017 WL 3972461, at *7.

Second, where allegations of redressability are stated plausibly, foreclosure of this remedy to Plaintiffs at this early juncture is not warranted. Expungement is a remedy that falls within the Court’s equitable discretion. *See United States v. Coloian*, 480 F.3d 47, 50 (1st Cir. 2007); *Reyes v. Supervisor of DEA*, 834 F.2d 1093, 1098 (1st Cir. 1984); *Chastain v. Kelley*, 510 F.2d 1232, 1235 (D.C. Cir. 1975) (stating that “federal courts are empowered to order the expungement of Government records where necessary to vindicate rights secured by the Constitution or by statute”). The availability of the remedy, therefore, depends upon the scope of the Defendants’ ultimate liability here. *See Janfeshan*, 2017 WL 3972461, at *13 (declining to dismiss the plaintiff’s “claims’ for CBP’s expungement of certain records” before determining the scope of the defendants’ liability); *Hassan v. City of N.Y.*, 804 F.3d 277, 293-94 (3d Cir. 2015) (explaining that “the potential avenues for redress depend on how a particular plaintiff’s injury shows itself” and may fall within a “range of available remedies”).

The Court thus DENIES Defendants' motion to dismiss on the basis that Plaintiffs lack standing to seek expungement.

B. Plaintiffs' Fourth Amendment Claims

The Fourth Amendment establishes that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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. The Fourth Amendment ensures that “the usual inferences which reasonable men draw from evidence be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.” *Johnson v. United States*, 333 U.S. 10, 14 (1948). “The amendment grew out of American colonial opposition to British search and seizure practices, most notably the use of writs of assistance, which gave customs officials broad latitude to search houses, shops, cellars, warehouses, and other places for smuggled goods.” *United States v. Wurie*, 728 F.3d 1, 3 (2013), *aff'd sub. nom.*, *Riley v. California*, ___ U.S. ___, 134 S. Ct. 2473 (2014).

“[T]he ultimate touchstone of the Fourth Amendment is reasonableness,” *Riley*, 134 S. Ct. at 2482 (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)), and “reasonableness generally requires the obtaining of a judicial warrant,” *id.* (quoting *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995)). “[A] warrantless search is *per se* unreasonable under the Fourth Amendment, unless one of ‘a few

specifically established and well-delineated exceptions’ applies.” *Wurie*, 728 F.3d at 3 (quoting *Arizona v. Gant*, 556 U.S. 332, 338 (2009)). 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).

Although, as an exception to the warrant requirement, border searches “have been considered to be ‘reasonable’ by the single fact that the person or item in question had entered into our country from outside,” *id.* at 619, the exception is not limitless. Border searches must still be “reasonable,” and the Court must still—as with searches conducted in the interior—balance “the sovereign’s interests” with the privacy interests of the individual. *United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985). Notably, however, the balance of interests is different at the border: the state has “a paramount interest in protecting[] its territorial integrity,” and an individual’s “expectation of privacy is less at the border than it is in the interior.” *United States v. Flores-Montano*, 541 U.S. 149, 153-54 (2004). That is, CBP and ICE argue that the ‘border is different’ from any other search context and there is no Fourth Amendment impediment to their policies.

By contrast, Plaintiffs argue that ‘digital is different.’ *See* D. 25 at 8.⁷ They contend that the

⁷ An amicus brief filed by the Brennan Center for Justice, the Center for Democracy & Technology, the R Street Institute and TechFreedom details the extent to which digital devices differ from containers at issue in prior border search cases given that they “contain great quantities of extremely

border searches at issue here run afoul of the Fourth Amendment due to the unique characteristics of electronic devices. D. 19 at 25-37. As to the border searches themselves, Plaintiffs argue that there is no meaningful distinction between basic and advanced (or manual and forensic) searches articulated in the CBP and ICE policies. D. 19 at 35. In light of the “the great volume and detail of personal information that electronic devices contain,” even manual searches, they allege, are “extraordinarily invasive.” D. 7 ¶ 41. See D. 7 ¶¶ 27-36. Plaintiffs allege (1) that the warrantless searches of travelers’ electronic devices conducted at the border or international ports of entry, pursuant to the CBP and ICE policies, violate the Fourth Amendment, and (2) that the confiscation of devices absent probable cause violates the Fourth Amendment. D. 7 ¶¶ 169, 173. The Court begins by focusing on Plaintiffs’ first Fourth Amendment claim, which applies to all Plaintiffs (Count I), and then addressing Plaintiffs’ confiscation claim which applies to certain of the Plaintiffs (Count III).

Six years ago, this Court was unpersuaded by the argument that, under Fourth Amendment jurisprudence, unique characteristics of cell phones and other electronic devices justified requiring a heightened level of suspicion for searches conducted at the border. *House v. Napolitano*, No. 11-10852-DJC, 2012 U.S. Dist. LEXIS 42297, 2012 WL 1038816, at *8 (D. Mass. Mar. 28, 2012). In *House*, similar to Plaintiffs here, House challenged the constitutionality of officers’ search of his laptop and other electronic devices at the border under the Fourth Amendment, arguing that the search was “highly intrusive given

sensitive information.” D. 25 at 7.

the personal nature and quality of information stored on these devices.” *Id.* at *6. The Court explained that in the Fourth Amendment context, “[i]t is the level of intrusiveness of the search that determines whether the search is routine, not the nature of the device or container to be searched.” *Id.* at *8 (citing *United States v. Giberson*, 527 F.3d 882, 888 (9th Cir. 2008)). The Court rejected House’s argument, explaining that a laptop and other electronic devices are “akin to the search of a suitcase and other closed containers,” which “require no particularized suspicion,” *id.* at *7, but declined to dismiss House’s Fourth Amendment claim because the prolonged detention of his electronic devices for forty-nine days was not “reasonably related in scope to the circumstances which justified it initially.” *Id.* at *9 (quoting *United States v. Cotterman*, 637 F.3d 1068, 1082 (9th Cir. 2011), *rev’d en banc*, 709 F.3d 952 (9th Cir. 2013)).

Two years after this Court’s ruling in *House*, as Plaintiffs point out, D. 19 at 25-31, the Supreme Court issued *Riley*, in which the Court held that the search-incident-to-arrest exception does not extend to cell phones, but rather the Fourth Amendment requires police to obtain a warrant supported by probable cause to search a phone seized during an arrest. *Riley*, 134 S. Ct. at 2494-95. Moreover, the Supreme Court in *Riley* affirmed the First Circuit’s ruling in *Wurie*, 728 F.3d at 13, which also came after this Court’s ruling in *House*.

1. *Riley, Wurie and the Search Incident to Arrest Exception*

In *Riley*, the Supreme Court addressed the applicability of the search incident to arrest exception to cell phones and established a categorical rule

requiring that officers obtain search warrants prior to searching cell phones. *Riley*, 134 S. Ct. at 2485. Justice Roberts, writing for a unanimous Court,⁸ explained that “[a]bsent more precise guidance from the founding era, we generally determine whether to exempt a given type of search 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 government interests.’” *Riley*, 134 S. Ct. at 2484 (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). The Court explained that the balancing of interests did not support extending the exception “to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.” *Id.*

The Court analyzed the rationales behind the search incident to arrest exception to determine whether application of the doctrine to “this particular category of effects would ‘untether the rule from the justifications underlying’” the exception. *Id.* at 2485 (quoting *Gant*, 556 U.S. at 343). Although the search incident to arrest exception has been described as “always recognized under English and American law,” *Weeks v. United States*, 232 U.S. 383, 392 (1914), it was not until 1969, in *Chimel v. California*, that the Supreme Court articulated the rationales behind the exception: removing weapons to ensure officer safety and preventing the destruction of evidence. *Chimel*, 395 U.S. 752, 762-63 (1969). Neither justification, the *Riley* Court explained, supported the application of

⁸ Justice Alito concurred in part and concurred in the judgment. *Riley*, 134 S. Ct. at 2495

the exception to cell phones. *Riley*, 134 S. Ct. at 2485-88. The Court rejected the government’s arguments that cell phones are “vulnerable to two types of evidence destruction unique to digital data—remote wiping and data encryption” because “broader concerns about the loss of evidence are distinct” from the rationale supporting the exception, the Court “ha[d] also been given little reason to believe that either problem is prevalent,” and it was unclear that the ability to conduct a cell phone search without a warrant would “make much of a difference.” *Id.* at 2486-87.

As to the individual’s privacy interests implicated, “[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.” *Id.* at 2488-89. The Supreme Court expounded at length upon the extent to which “[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee’s person.” *Id.* at 2489. Quantitatively, whereas “[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,” cell phones have an “immense storage capacity,” allowing people to carry an amount of data no longer limited by physical practicability. *Id.* “The sum of an individual’s private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions” dating back to the purchase of the phone, or earlier; “the same cannot be said of a photograph or two of loved ones tucked into a wallet.” *Id.* Qualitatively, a person’s

internet browsing history, historic location information, and mobile application software (or “apps”) “can form a revealing montage of the user’s life.” *Id.* at 2490. Indeed, the Court stated that “a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house.” *Id.* at 2491 (emphasis in original). Moreover, the ease with which a cell phone may be used to access remote files illustrates that a cell phone search “might extend well beyond papers and effects in the physical proximity of an arrestee,” providing “yet another reason that the privacy interests here dwarf those” in prior search incident to arrest cases. *Id.*

The *Riley* court rejected the government’s proposed alternative standards, including that “from the vehicle context, allowing a warrantless search of an arrestee’s cell phone whenever it is reasonable to believe that the phone contains evidence of the crime of arrest.” *Id.* at 2492. The Supreme Court explained that the exception for warrantless searches of a vehicle’s passenger compartment carved out in *Gant*, 556 U.S. at 343, was inapplicable to cell phone searches for several reasons. *Riley*, 134 S. Ct. at 2492. First, the circumstances of the vehicle search involved further “reduced expectation[s] of privacy” and “heightened law enforcement needs” absent with cell phone searches. *Id.* (quoting *Thornton v. United States*, 541 U.S. 615, 632 (2004) (Scalia, J., concurring)); see *Gant*, 556 U.S. at 345. Second, crucially, the “*Gant* standard would prove no practical limit at all when it comes to cell phone searches,” given the physical and temporal limitations present in a *Gant* scenario that are absent in a *Riley* scenario.

Riley, 134 S. Ct. at 2492. The Court noted that “[i]t would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone.” *Id.* Given the Court’s “general preference to provide clear guidance to law enforcement through categorical rules,” and avoid “a difficult line-drawing expedition” for officers and courts alike, the Court rejected the government’s “fallback options” in favor of a warrant requirement that would apply to all cell phone searches conducted incident to arrest. *Id.* at 2491-93; *see id.* at 2497 (Alito, J., concurring) (explaining that although the Court’s holding might “lead[] to anomalies,” he did “not see a workable alternative” given that “[l]aw enforcement officers need clear rules . . . and it would take many cases and many years for the courts to develop more nuanced rules”).

It is also worth noting that one of the two cases on appeal in *Riley* was *Wurie*, a 2013 First Circuit opinion reversing the denial of a motion to suppress and holding that cell phones are distinct from other physical possessions that may be searched incident to arrest without a warrant. *Wurie*, 728 F.3d at 13-14. The First Circuit pointed to Seventh Circuit case law acknowledging that “[a]t the touch of a button a cell phone search becomes a house search, and that is not a search of a ‘container’ in any normal sense of that word, though a house contains data.” *Id.* at 8-9 (quoting *United States v. Flores-Lopez*, 670 F.3d 803, 806 (7th Cir. 2012)). Ultimately, however, the First Circuit parted ways with the Seventh Circuit and a “majority” of jurisdictions that had upheld warrantless cell phone data searches. *Id.* at 5, 13. The

First Circuit concluded instead that cell phone searches incident to arrest are not justified by the *Chimel* rationales, and that the nature and scope of the search exceeded the purposes of the warrant exception. *Id.* at 7-12. The court explained that cell phones store “much more personal information . . . than could ever fit in a wallet, address book, briefcase, or any of the other traditional containers that the government has invoked.” *Id.* at 9.

Adhering to “the Supreme Court’s insistence on bright-line rules in the Fourth Amendment context,” the First Circuit explained that while some searches of cell phones might be less invasive than others, “it is necessary for all warrantless cell phone data searches to be governed by the same rule.” *Id.* at 12-13. In the court’s view, the government’s desire for warrantless cell phone searches was “a convenient way for the police to obtain information related to a defendant’s crime of arrest,” and the court found no Supreme Court jurisprudence sanctioning “such a ‘general evidence-gathering search.’” *Id.* at 13 (quoting *Thornton*, 541 U.S. at 632 (Scalia, J., concurring)). The First Circuit likened the government’s proposed approach to “customs officers in the early colonies [who] could use writs of assistance to rummage through homes and warehouses, without any showing of probable cause linked to a particular place or item sought,” the very ill the Founders sought to eradicate with the Fourth Amendment. *Id.* at 9. In *Riley*, the Supreme Court affirmed the First Circuit’s ruling. *Riley*, 134 S. Ct. at 2495.

2. *Riley and the Border Search Exception*

Defendants argue that *Riley* does not apply to the border search context. D. 15 at 25-27. Defendants

state that “*Riley* itself noted that its holding was limited to the search incident to arrest context” by acknowledging that “other case-specific exceptions may still justify a warrantless search of a particular phone.” D. 15 at 26 (quoting *Riley*, 134 S. Ct. at 2492). On that basis, Defendants contend, the argument that *Riley* “imposes a warrant requirement” in the border search context “is without merit and has been repeatedly rejected.” D. 15 at 25. Additionally, and more substantively, Defendants contend that, unlike the rationales behind the search incident to arrest exception, the border search exception “serves different and broader purposes” that “apply in full force to searches of electronic media.” D. 15 at 26-27.

As an initial matter, the Court is not persuaded that *Riley*’s reasoning is irrelevant here simply because *Riley*’s holding was limited to the search incident to arrest exception, *see Riley*, 134 S. Ct. at 2495. Judicially recognized exceptions to the warrant requirement do not exist in isolation; rather, they are all part of Fourth Amendment jurisprudence, justified because, ordinarily, the circumstances surrounding the search and the nature of the search have been deemed “reasonable.” *See id.* at 2483; *Ramsey*, 431 U.S. at 617. In fact, the Supreme Court has referenced search incident to arrest doctrine within its border search jurisprudence in the past, characterizing the two exceptions as “similar.” *Ramsey*, 431 U.S. at 621 (explaining that the border search is “a longstanding, historically recognized exception to the Fourth Amendment’s general principle that a warrant be obtained, and in this respect is like the similar ‘search incident to lawful arrest’ exception”). The reasoning in *Riley* may, therefore, carry some persuasive weight in

the border search context. *See, e.g., United States v. Kolsuz*, 185 F. Supp. 3d 843, 856 (E.D. Va. 2016) (considering scope of privacy interest at border in light of *Riley*); *United States v. Kim*, 103 F. Supp. 3d 32, 54-58 (D.D.C. 2015) (same); *cf. United States v. Camou*, 773 F.3d 932, 942-43 (9th Cir. 2014) (extending *Riley* to the vehicle exception context); *United States v. Lara*, 815 F.3d 605, 610-12 (9th Cir. 2016) (applying *Riley* to probation search context); *United States v. Henry*, 827 F.3d 16, 28 (1st Cir. 2016) (rejecting defendant’s *Riley* argument in the “plain view” context not because *Riley* was categorically irrelevant but because the officers had obtained a warrant prior to the smart phone search).

Additionally, the cases Defendants reference to argue that Plaintiffs’ Fourth Amendment claim has been “repeatedly rejected,” D. 15 at 26 n.8, carry limited weight here. The majority of these cases arose in district courts within the Ninth Circuit, where *Cotterman*, 709 F.3d at 968, a Ninth Circuit *en banc* decision predating *Riley*, still controls. *See, e.g., United States v. Mendez*, 240 F. Supp. 3d, 1005, 1008 (D. Ariz. 2017); *United States v. Ramos*, 190 F. Supp. 3d 992, 1002-03 (S.D. Cal. 2016); *United States v. Lopez*, No. 13-CR-2092 WQH, 2016 U.S. Dist. LEXIS 176920, 2016 WL 7370030, at *5 (S.D. Cal. Dec. 20, 2016). In *Cotterman*, the Ninth Circuit held that a forensic device search initiated at the border required reasonable suspicion, explaining that “the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property.” *Cotterman*, 709 F.3d at 966. Lower courts in the Ninth

Circuit are bound by the *Cotterman* standard, unable to apply *Riley* in the border context unless they find the two cases “clearly irreconcilable,” which, as several courts have explained, they are not. See *United States v. Caballero*, 178 F. Supp. 3d 1008, 1018 (S.D. Cal. 2016) (explaining that “[a]lthough *Riley* could be applied to a cell phone search at the border, this Court is bound by *Cotterman*”); *Lopez*, 2016 WL 7370030, at * 5.⁹

Here, the First Circuit has not yet spoken on what level of suspicion is required to justify a cell phone or other electronic device search at the border. The First Circuit has, however, acknowledged the significant privacy interests implicated in a cell phone search, explaining that the information on these devices is “the kind of information one would previously have stored in one’s home and that would have been off-limits to officers performing a search incident to arrest.” *Wurie*, 728 F.3d at 8. Searches of cell phones are fundamentally different from “the kinds of reasonable, self-limiting searches that do not offend the Fourth Amendment, even when conducted without a warrant.” *Id.* at 9-10. The court also emphasized the necessity behind a bright-line rule favoring a warrant requirement, explaining that “[a] series of opinions allowing some cell phone data searches but not others, based on the nature and reasonableness of the intrusion, would create exactly

⁹ Likewise, district courts in the Fourth Circuit are bound by pre-*Riley* precedent in *United States v. Ickes*, in which the Fourth Circuit held that a manual digital search of an electronic device is a routine border search, requiring no individualized suspicion, *Ickes*, 393 F.3d 501, 505-06 (4th Cir. 2005). See *Kolsuz*, 185 F. Supp. 3d at 854-55; *United States v. Saboonchi*, 990 F. Supp. 2d 536, 560 (D. Md. 2014).

the ‘inherently subjective and highly fact specific’ set of rules that the Court has warned against and would be extremely difficult for officers in the field to apply.” *Id.* at 12-13 (quoting *Thornton*, 541 U.S. at 623).

While it is correct that neither the Supreme Court nor the First Circuit have yet held that a warrant is required for a particular type of search conducted at the border, the Court considers Plaintiffs’ claim against the current legal backdrop framed by *Riley* and *Wurie* and thus turns to the merits to determine whether Plaintiffs have plausibly alleged a Fourth Amendment violation for warrantless border device searches.

The border search exception is widely considered as old as the United States itself. *See Ramsey*, 431 U.S. at 616-17. “The Congress which proposed the Bill of Rights, including the Fourth Amendment, to the state legislatures on September 25, 1789, 1 Stat. 97, had, some two months prior to that proposal, enacted the first customs statute, Act of July 31, 1789, c. 5, 1 Stat. 29 grant[ing] customs officials ‘full power and authority’ to enter and search ‘any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed.” *Id.* at 616. The Supreme Court reiterated in 1886 and 1925 that border searches are “reasonable” and, therefore, not prohibited by the Fourth Amendment. *See Boyd v. United States*, 116 U.S. 616, 623 (1886); *Carroll v. United States*, 267 U.S. 132, 147 (1925).

As with all Fourth Amendment exceptions, the border search exception is “subject to substantive limitations imposed by the Constitution.” *Ramsey*, 431 U.S. at 620. The Court determines “the permissibility

of a particular law enforcement practice . . . by balancing its intrusion on the individual's Fourth Amendment interest against its promotion of legitimate governmental interests.” *Montoya de Hernandez*, 473 U.S. at 537 (quoting *United States v. Villamonte-Marquez*, 462 U.S. 579, 588 (1983)). “[T]he Fourth Amendment’s balance of reasonableness is qualitatively different at the international border than in the interior.” *Id.* at 538. 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 154, 152.

The border search slate, however, is not unlike the one on which the Supreme Court wrote in *Riley*. Like the border search exception’s historical foundation, the search incident to arrest exception, as the Court detailed in *Riley*, was “always recognized under English and American law,” *Riley*, 134 S. Ct. at 2482 (quoting *Weeks*, 232 U.S. at 392). Moreover, with searches incident to arrest, the balance also tilts favorably toward the government. *See id.* at 2488 (explaining that “[t]he search incident to arrest exception rests not only on the heightened government interests at stake in a volatile arrest situation, but also on an arrestee’s reduced privacy interests upon being taken into police custody”). The Court nevertheless explained that an arrestee’s “diminished privacy interests do[] not mean that the Fourth Amendment falls out of the picture entirely.” *Id.* Rather, the unique attributes of cell phones so increased the privacy interests of individuals that the balancing of interests that typically support the

search incident to arrest exception no longer applied. *See id.* at 2484-85, 2488; *Wurie*, 728 F.3d at 9.

The border search serves the nation’s “paramount interest in protect[ing] 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.

Plaintiffs argue that “warrantless searches of electronic devices are not sufficiently tethered to the narrow purposes justifying the border search exception: immigration and customs enforcement.” D. 19 at 28-29. If the border exception seeks to enable officers to prevent illicit “contraband” from entering the country, *see Montoya de Hernandez*, 473 U.S. at 537, a search of digital data may not be necessary to achieve that aim. *See Kolsuz*, 185 F. Supp. 3d at 858 (explaining that digital information “is merely indirect evidence of things an individual seeks to

export illegally—not the things themselves—and therefore the government’s interest in obtaining this information is less significant than the government’s interest in directly discovering the items to be exported illegally”); *United States v. Molina-Isidoro*, 267 F. Supp. 3d 900, 909 n.10 (W.D. Tex. 2016). Defendants argue that devices “can contain contraband (such as child pornography), information regarding the inadmissibility of prohibited goods or persons, or material (such as classified information, malware, or export-controlled material) that, if illicitly transferred beyond our borders, could pose a direct threat to our national security.” D. 15 at 27. The Court agrees with Plaintiffs that “information regarding the inadmissibility of prohibited goods or persons,” *id.*, is distinct from contraband. D. 19 at 30 n.20; *see Boyd*, 116 U.S. at 623 (explaining that search and seizure of “goods liable to duties and concealed to avoid the payment thereof[] are totally different things from a search for and seizure of a man’s private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him”).

Digital contraband like child pornography, however, falls within the ambit of the border search exception’s rationales. Plaintiffs argue that unlike physical contraband, digital contraband may also cross borders digitally, through the internet, and need not physically cross the border to enter the country. D. 19 at 30. Additionally, they argue that to the extent such digital contraband is truly transported across the border through these devices, the government cannot demonstrate that such incidents are “prevalent” enough to justify a categorical rule permitting

warrantless device searches at the border. *Id.* (quoting *Riley*, 134 S. Ct. at 2486). The U.S. Sentencing Commission explained in 2012 that “[t]he vast majority of child pornography offenders today use the Internet or Internet-related technologies to access and distribute child pornography.” U.S. Sent’g Comm’n, *2012 Report to the Congress: Federal Child Pornography Offenses* 41-42 (2012)¹⁰; see *id.* at 48-56 (describing peer-to-peer file sharing and other platforms enabling file sharing on the internet). With the limited record before the Court, the prevalence of physical transfers of illicit digital contraband across the U.S. borders (as opposed to through the internet) is unclear.

Additionally, although the Court agrees with Defendants that digital contraband is not “untethered” from the rationales supporting the border search exception, it is unclear at this juncture the extent to which a warrant requirement would impede customs officers’ ability to ferret out such contraband.¹¹ “[T]he mere fact that law enforcement may be made more efficient can never by itself justify

¹⁰ Available online at http://www.ussc.gov/sites/default/files/pdf/news/congressional-testimony-and-reports/sex-offense-topics/201212-federal-child-pornography-offenses/Full_Report_to_Congress.pdf.

¹¹ One district court explained, prior to *Riley*, in holding that forensic searches require reasonable suspicion, such a ruling is not “likely meaningfully to change anything that actually happens at the border,” because “[c]ustoms officials do not have the time or resources—or, most likely, the inclination—to perform random or suspicionless forensic searches.” *Saboonchi*, 990 F. Supp. 2d at 570. The court was unaware of “any case where a forensic search was performed in the absence of reasonable suspicion.” *Id.* (citing cases).

disregard of the Fourth Amendment.” *Wurie*, 728 F.3d at 11 (quoting *Mincey v. Arizona*, 437 U.S. 385, 393 (1978)). Indeed, as Justice Roberts pointed out in *Riley*, “[r]ecent technological advances similar to those discussed here have, in addition, made the process of obtaining a warrant itself more efficient.” *Riley*, 134 S. Ct. at 2493. Although a warrant might “have an impact on the ability of law enforcement to combat crime,” *id.*, it is unclear—based on the record before the Court at this time—the extent to which such impediment justifies applying the border search exception to electronic devices. This is particularly true where the government’s interests—even if they are not “untethered” to the exception’s rationales—must be “[w]eighed against the significant privacy implications inherent in cell phone data searches.” *Wurie*, 728 F.3d at 11.

On the other side of the scale, where a traveler’s privacy interests are ordinarily reduced, *Riley* indicates that electronic devices implicate privacy interests in a fundamentally different manner than searches of typical containers or even searches of a person. *Riley*, 134 S. Ct. at 2488-89, 2494-95; see *Wurie*, 728 F.3d at 8. The Supreme Court has held that detention of a traveler at the border “beyond the scope of a routine customs search and inspection” may be justified when supported by reasonable suspicion that the traveler is smuggling contraband in their “alimentary canal,” *Montoya de Hernandez*, 473 U.S. at 541, and that no level of suspicion is required for a border search in which officers “remove, disassemble, and reassemble a vehicle’s fuel tank,” *Flores-Montano*, 541 U.S. at 155. The First Circuit, likewise, has held that reasonable suspicion—not probable cause—is

required to justify certain “nonroutine” border examinations like strip and body cavity searches. *United States v. Braks*, 842 F.2d 509, 512-14 (1st Cir. 1988). The First Circuit and other circuits have adopted the “routine” and “nonroutine” border search distinction first articulated in *Montoya de Hernandez*, 473 U.S. at 541 n.4, often distinguishing between the two by the intrusiveness of the search. See *United States v. Molina-Gómez*, 781 F.3d 13, 19 (1st Cir. 2015); *United States v. Kelly*, 302 F.3d 291, 294 (5th Cir. 2002); *United States v. Ramos-Saenz*, 36 F.3d 59, 61 (9th Cir. 1994).¹²

Riley and *Wurie* indicate that electronic device searches are, categorically, more intrusive than searches of one’s person or effects. See *Riley*, 134 S. Ct. 2489 (explaining 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”); *Wurie*, 728 F.3d at 8-9; *United States v. Whiteside*, No. 13-cr-576, 2015 U.S. Dist. LEXIS 84369, 2015 WL 3953477, at *4-5 (S.D.N.Y. June 29, 2015) (suppressing contents of digital camera searched incident to arrest based upon *Riley*). The ability to review travelers’ cell phones allows officers to view “nearly every aspect of their lives—from the

¹² The Supreme Court’s dismissal of the “[c]omplex balancing tests” to determine the “degree of intrusiveness” as applied to border searches of vehicles, *Flores-Montano*, 541 U.S. at 152, does not eliminate the intrusiveness inquiry here. There, the Court explained that the “dignity and privacy interests of the person being searched [] simply do not carry over to vehicles.” *Id.*; see *New York v. Class*, 475 U.S. 106, 112-13 (1986) (explaining that vehicles implicate a diminished expectation of privacy). Under current Supreme Court jurisprudence, the opposite holds true for cell phones. See *Riley*, 134 S. Ct. at 2489-90.

mundane to the intimate.” *Riley*, 134 S. Ct. at 2490. Indeed, certain facts alleged here—including Nadia Alasaad’s and Merchant’s objections due to their photos on their phones of themselves without headscarves, D. 7 ¶¶ 67, 129—demonstrate the level of intrusiveness a manual device search can entail. The Constitutional Accountability Center, in its *amicus* brief, likens digital device searches to searches of personal papers, explaining that “personal papers increasingly take the form of digital files” kept on cell phones, laptops, and other electronic devices. D. 23 at 8. They argue personal papers require greater protection under the Fourth Amendment because these searches “go[] to the very core of the fourth amendment right of privacy,” given the Fourth Amendment’s history and the “inherently ‘personal, private nature of such papers.” D. 23 at 18 (quoting James A. McKenna, *The Constitutional Protection of Private Papers: The Role of a Hierarchical Fourth Amendment*, 53 Ind. L.J. 55, 68 (1977)); see Craig M. Bradley, *Constitutional Protection for Private Papers*, 16 Harv. C.R.-C.L. L. Rev. 461, 483 (1981) (describing the “psychological intrusion” implicated by searches of personal papers “because the searcher is invading not only the subject’s house but his or her thoughts as well”); *Ramsey*, 431 U.S. at 623-24 (holding that searches for contraband in international mail did not violate the Fourth Amendment, repeatedly stressing that statutes forbade reading correspondence in the envelopes). Moreover, the potential intrusion into individuals’ privacy is of “particular concern” in the border search context because the permissible scope of customs officers’ investigative search is so broad and need not “be restrained by any limitations of exigency or relevance to a specific crime.” *Camou*, 773 F.3d at

943 (explaining that the broad “allowable scope” of a search pursuant to the vehicle exception supported extending *Riley*’s holding to cell phone searches in that context).

Defendants argue that even if device searches necessitate heightened suspicion, not higher standard could apply here than the reasonable suspicion standard.¹³ D. 15 at 25; see *Molina-Gómez*, 781 F.3d at 19 (explaining that non-routine searches “require reasonable suspicion”). Plaintiffs argue, however, that the Supreme Court has never suggested that reasonable suspicion “is a ceiling for every border search.” D. 19 at 33. Defendants emphasized at oral argument that First Circuit precedent has never required that strip searches in the border context meet a standard higher than reasonable suspicion, see *Braks*, 842 F.2d at 512-14, so holding digital searches to a higher standard would be incongruous. See D. 32 at 6. Notably, however, reasonable suspicion generally suffices to justify strip searches in the search incident to arrest context, too. See *United States v. Barnes*, 506 F.3d 58, 62 (1st Cir. 2007); *Swain v. Spinney*, 117 F.3d 1, 7 (1st Cir. 1997).¹⁴ Nevertheless, the Supreme Court

¹³ Reasonable suspicion is generally defined as “a particularized and objective basis for suspecting the particular person stopped of criminal activity.” *United States v. Cortez*, 449 U.S. 411, 417-18 (1981); *Terry v. Ohio*, 392 U.S. 1, 21, 30 (1968) (explaining that the standard is met when officers can point to “specific and articulable facts” and rational inferences that can be drawn therefrom indicating that criminal activity “may be afoot”). It is typically viewed within the totality of the circumstances. See *Cortez*, 449 U.S. at 417.

¹⁴ Notably, in *Swain*, the First Circuit again connected the search incident to arrest exception with the border search exception, explaining that the reasonable suspicion standard was

rejected the reasonable suspicion standard when it came to cell phones because it “would prove no practical limit at all when it comes to cell phone searches.” *Riley*, 134 S. Ct. at 2492. Digital device searches at the border, perhaps even when supported by reasonable suspicion, raise the same concerns.

In sum, the Court is not persuaded that Plaintiffs have failed to state a plausible Fourth Amendment claim here. Although Defendants may be correct that the border is different, *see* D. 15 at 23-27, the Supreme Court and First Circuit have acknowledged that digital searches are different too since they “implicate privacy concerns far beyond those implicated” in a typical container search. *Riley*, 134 S. Ct. at 2488-89; *see Wurie*, 728 F.3d at 11. In the absence of controlling precedent to the contrary, this Court cannot rule that this Fourth Amendment principle would not extend in some capacity to the border. *See Janfeshan*, 2017 WL 3972461, at *12 (denying motion to dismiss Fourth Amendment claim regarding forensic cell phone search at border); *Kim*, 103 F. Supp. 3d at 59 (granting motion to suppress where forensic laptop search “was supported by so little suspicion of ongoing or imminent criminal activity, and was so invasive of Kim’s privacy . . . that it was unreasonable” under the Fourth Amendment and *Riley*); *United States v. Djibo*, 151 F. Supp. 3d 297, 310 (E.D.N.Y. 2015) (granting motion to suppress documents obtained from warrantless search of phone of outbound passenger under *Riley*). The Court concludes, therefore, that Plaintiffs have plausibly alleged a Fourth Amendment claim here.

appropriate for strip and visual body cavity searches in the arrestee context because it was appropriate in other contexts, including “non-routine border searches.” *Swain*, 117 F.3d at 7.

Plaintiffs also argue that even if *Riley* does not apply here, “border search precedent provides a parallel justification for requiring a warrant based on probable cause for border searches of electronic devices.” D. 19 at 31. Given that the Court has concluded that *Riley* has some weight in the border search context and that, on that basis, Plaintiffs have stated a plausible Fourth Amendment claim, the Court need not reach this further argument.

Defendants’ motion to dismiss Plaintiffs’ Fourth Amendment claim (Count I) is, therefore, DENIED.

3. *Plaintiffs’ Confiscation Claim*

Defendants also seek dismissal of Plaintiffs’ claim that Defendants “violate the Fourth Amendment by confiscating travelers’ electronic devices, for the purpose of effectuating searches of those devices after travelers leave the border, absent probable cause” as they are “unreasonable at their inception, and in scope and duration,” D. 7 ¶ 173. D. 14 at 2; D. 15 at 30-34. Defendants contend that “[t]he same arguments made with respect to the first cause of action . . . apply equally here,” arguing that “where the government has authority to search an item at the border, it has authority to detain that item as necessary to accomplish the search.” D. 15 at 30-31. To the extent this standard is correct—which the Court does not grant—given this Court’s ruling on Plaintiffs’ Fourth Amendment claim regarding border device searches, and for many of the reasons detailed above, the Court likewise holds that Plaintiffs have plausibly alleged a Fourth Amendment claim based upon Defendants’ prolonged detention—or confiscation—of these devices.

The Court notes, moreover, that Plaintiffs' claim pertaining to confiscations is not coterminous with Plaintiffs' border search claim. Unlike border searches, prolonged detentions of devices—including after travelers have left the border—resemble seizures, and must, therefore, be reasonable not only at their inception but also for their duration. *United States v. Place*, 462 U.S. 696, 708-10 (1983) (holding that the ninety-minute detention of luggage was a “seizure” requiring probable cause); see *United States v. Jacobsen*, 466 U.S. 109, 124-25 (1984). That is, a device search that is justified at its inception may nevertheless become unreasonable, giving rise to a Fourth Amendment claim. See *House*, 2012 WL 1038816, at *10 (holding that a forty-nine day detention of a locked laptop, flash drive and camera raised a plausible Fourth Amendment claim, despite dismissing claim regarding the search itself); *Cotterman*, 709 F.3d at 966-67.

Plaintiffs argue that confiscations pursuant to CBP and ICE policies are “excessive” in scope and duration. D. 7 ¶¶ 56(b)-(c). As this Court has previously explained, “the inquiry into the reasonableness of the duration of a seizure is . . . an appropriate consideration under the Fourth Amendment analysis” even at the border. *House*, 2012 WL 1038816, at *9 (citing *Place*, 462 U.S. at 709-10); see *United States v. Mitchell*, 565 F.3d 1347, 1351-52 (11th Cir. 2009) (holding that a twenty-one day delay in securing a warrant for a laptop search was unreasonable). Defendants argue that Plaintiffs' claim is baseless given that the official policies limit detentions to “a brief, reasonable period of time.” D. 15 at 34 (quoting D. 18-1 ¶ 5.3.1). The lengths of the

detentions alleged here, however—including ten months for Allababidi and fifty-six days for Wright—suggest that the Fourth Amendment may require clearer guidance than that. *See Riley*, 134 S. Ct. at 2492-93 (reiterating the necessity of “clear guidance” in the Fourth Amendment context).

The Court thus DENIES Defendants’ motion to dismiss Plaintiffs’ Fourth Amendment claim regarding confiscation of electronic devices pursuant to CBP and ICE policies (Count III).

C. Plaintiffs’ First Amendment Claim

Finally, Defendants seek dismissal of Plaintiffs’ claim, Count II, that they “violate the First Amendment by searching electronic devices that contain expressive content and associational information, absent a warrant supported by probable cause,” D. 7 ¶ 171. D. 14 at 2. 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. These rights “are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference.” *Bates v. City of Little Rock*, 361 U.S. 516, 523 (1960). As the Supreme Court has explained, “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”).

Plaintiffs argue that warrantless digital device searches substantially burden travelers’ protected rights of freedom of speech and association and chill the exercise of these rights. D. 7 ¶ 46; D. 19 at 38-41; *see generally* D. 26 (*amicus* brief filed by the Knight First Amendment Institute at Columbia University and the Reporters Committee for Freedom of the Press). They explain that the First Amendment rights implicated include the “right to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends,” *Roberts v. U.S. Jaycees*, 468 U.S. 609, 622 (1984); *see NAACP v. Alabama*, 357 U.S. 449, 460 (1958), the right to publish speech anonymously, *see McIntyre v. Ohio Elections Cmm’n*, 514 U.S. 334, 351-43; *McMann v. Doe*, 460 F. Supp. 2d 259, 266 (D. Mass. 2006), and the right to communicate privately, *see Lamont v. Postmaster Gen.*, 381 U.S. 301, 305 (1965). D. 19 at 38. Freedom of the press is also implicated here, as with Plaintiffs Dupin and Kushkush. D. 19 at 39; D. 26 at 11-13; *see Bruno & Stilman, Inc. v. Globe Newspaper Co.*, 633 F.2d 583, 595-96 (1st Cir. 1980).

Plaintiffs argue that to justify digital device searches, “[t]he government must have a compelling interest in the information and use narrowly tailored means that do not seek more information than necessary.” D. 19 at 38. The Court is not convinced that such strict scrutiny applies here, where CBP and ICE policies are content-neutral, *see Asociacion de Educacion Privada de P.R., Inc. v. Garcia-Padilla*, 490

F.3d 1, 15-16 (1st Cir. 2007), and, although potentially burdening speech, do not prevent anyone from speaking, *Sindicato Puertorriqueño de Trabajadores v. Fortuño*, 699 F.3d 1, 12 (1st Cir. 2012). In general, however, compelled disclosure of First Amendment protected activity “cannot be justified by a mere showing of some legitimate governmental interest.” *Buckley v. Valeo*, 424 U.S. 1, 64 (1976). Rather, “even if any deterrent effect on the exercise of First Amendment rights arises, not through direct government action, but indirectly as an unintended but 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; see *Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 546 (1963). The Court must, therefore, determine whether the complaint adequately alleges an interference with First Amendment rights that is “direct and substantial” or “significant.” *House*, 2012 WL 1038816, at *12 (quoting *Fighting Finest v. Bratton*, 95 F.3d 224, 228 (2d Cir. 1996)). Plaintiffs argue that given the technological capacities of electronic devices, the government’s broad search policies “impose[] a substantial burden on First Amendment rights without justification.” D. 19 at 41.

Defendants do not argue that warrantless searches would not be a significant or substantial burden on travelers’ First Amendment rights, nor do they explain their assertion that a heightened standard is not “required by the First Amendment.” D. 32 at 6 n.4. Rather, Defendants argue that “the border search doctrine is not subject to a First Amendment exception,” and that if it were, the

consequences would be “staggering.” D. 15 at 29 (quoting *Ickes*, 393 F.3d at 507, 506). As a general matter, “[t]hat the initial search and seizure occurred at the border does not strip [Plaintiffs] of [their] First Amendment rights.” *House*, 2012 WL 1038816, at *13; *Tabbaa*, 509 F.3d at 102 n.4 (explaining that a routine search may constitute a “significant or substantial burden on plaintiffs’ First Amendment associational rights”).

Moreover, the Court is not persuaded that *Ickes*, 393 F.3d at 506, upon which Defendants rely, provides appropriate guidance here. This Court need not carve out an exception for all expressive material to find a plausible claim has been stated that digital device searches unjustifiably burden travelers’ First Amendment rights. *See House*, 2012 WL 1038816, at *13 (holding that the plaintiff stated plausible First Amendment claim for his cell phone search despite failing to state plausible Fourth Amendment claim). The Supreme Court’s distinction between cell phones and other expressive materials in *Riley*, postdating the Fourth Circuit’s ruling in *Ickes*, further illustrates this point. *See Riley*, 135 S. Ct. at 2490. Additionally, in *Ickes*, the Fourth Circuit was concerned with the “headaches” such a First Amendment “exception” would bring for customs officers. *Ickes*, 393 F.3d at 506. What Plaintiffs seek as a remedy here, however, is “simple—get a warrant,” *Riley*, 134 S. Ct. at 2495. D. 19 at 39. Finally, in *Ickes*, the Fourth Circuit assured that the defendant’s warning that “any person carrying a laptop computer . . . on an international flight would be subject to a search of the files on the computer hard drive” was “far-fetched,” *Ickes*, 393 F.3d at 506-07. Plaintiffs point to the recent

increase in border device searches and the expanding storage and functioning capacities of electronic devices to suggest otherwise. D. 7 ¶¶ 30, 38; D. 19 at 41.

Defendants also argue that this Court’s reasoning in *House* does not apply here. D. 15 at 29. They contend that “the facts of that case are easily distinguished,” where, unlike here, House alleged he was targeted for investigation because of his specific expressive or associational activities. *Id.*; see *House* 2012 WL 1038816, at *10-11. First, certain Plaintiffs allege facts prior to their device searches that are not dissimilar to those in *House*: while Dupin’s phone was being searched, he was questioned “about his work as a journalist, including the names of the organizations and specific individuals within those organizations for whom he had worked”; Gach was questioned “about his work as an artist” prior to searching his phone; Kushkush was asked about “his reporting activities”; and Merchant was questioned at secondary inspection about her “religious affiliation” and her blog. D. 7 ¶¶ 87, 93, 99, 109, 133. One *amicus* argues that journalists “are particularly vulnerable to targeted surveillance by means of suspicionless device searches.” D. 26 at 13. As in *House*, such allegations are “pertinent” to Plaintiffs’ First Amendment claim because they suggest that the officers’ “motivation to search and retain [Plaintiffs’] devices” was to examine expressive or associational material. *House*, 2012 WL 1038816, at *10.

Second, the reasoning in *House* was not limited to targeting allegations alone. The Court explained there that the seizure of House’s laptop and other devices gave the government possession of

confidential lists of organizational members and supporters, as well as emails and documents detailing House’s organization’s inner workings. *House*, 2012 WL 1038816, at *12. Such “[c]ompulsory disclosure . . . ‘can seriously infringe on privacy of association and belief guaranteed by the first amendment,’ and can ‘have . . . a profound chilling effect.’” *Id.* (quoting *Buckley*, 424 U.S. at 64; *Perry v. Schwarzenegger*, 591 F.3d 1126, 1135 (9th Cir. 2009)) (internal citations omitted). Here, the CBP and ICE policies broadly permit suspicionless searches in pursuit of “information,” ICE Pol. ¶¶ 5.2, 6.1; D. 18-2 ¶ 5.1.3, which could reasonably include such searches within their ambit. In *Ramsey*, as Plaintiffs point out, D. 19 at 40, the Supreme Court held that the statutory scheme permitting warrantless search of incoming international mail did not violate the constitution because it applied only when there was reason to believe the envelopes contained physical items and regulations “flatly prohibit[ed], under all circumstances,” customs officials from reading correspondence without a warrant. *Ramsey*, 431 U.S. at 623. The Court did not “decide whether, in the absence of the regulatory restrictions, 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 624 n.18. Here, there are no similar First Amendment safeguards in the CBP and ICE electronic device policies.

In light of the particular concerns raised by digital devices like cell phones detailed above, *see Riley*, 134 S. Ct. at 2489-91, and the limitless search authorizations in the CBP and ICE policies, Plaintiffs have plausibly alleged that the government’s digital

device search policies substantially burden travelers' First Amendment rights.¹⁵

The Court, therefore, declines to dismiss Plaintiffs' First Amendment claim (Count II).

VI. Conclusion

For the foregoing reasons, the Court DENIES Defendants' motion to dismiss, D. 14.

So Ordered.

/s/ Denise J. Casper
United States District Judge

¹⁵ The Court also notes that Plaintiffs' Fourth and First Amendment claims are closely related. *See Janfeshan*, 2017 WL 3972461, at *12 (declining to dismiss plaintiff's Fourth Amendment claim after denying dismissal of his Fifth Amendment claim because they were "integrally related," and discovery would "involve the same witnesses and w[ould] largely overlap").

APPENDIX E

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

No. 17-cv-11730-DJC

GHASSAN ALASAAD, et al.,

Plaintiffs,

v.

KEVIN McALEENAN, Secretary of the U.S.
Department of Homeland Security, in his official
capacity, et al.,

Defendants.

Hon. DENISE J. CASPER

July 12, 2019

**PLAINTIFFS' SUPPLEMENTAL STATEMENT
OF UNDISPUTED MATERIAL FACTS**

Plaintiffs hereby submit their Supplemental Statement of Undisputed Material Facts in support of their Motion for Summary Judgment, ECF No. 90, and in opposition to Defendants' motion for summary judgment, ECF No. 96.

**PLAINTIFF’S SUPPLEMENTAL STATEMENT
OF UNDISPUTED MATERIAL FACTS**

125.1. On July 6, 2019, Suhaib Allababidi arrived at the Toronto airport for a flight to Dallas. Exh. 52 (7/11/19 Allababidi Dec.) at ¶ 1. He traveled with a smartphone and a laptop. *Id.* at ¶¶ 3-4, 7-8. At the Toronto preclearance area, U.S. Customs and Border Protection (“CBP”) searched both Allababidi’s phone and laptop. *See id.* at ¶¶ 3-10.

Respectfully submitted:

Dated: July 12, 2019

/s/ Saira Hussain

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

Esha Bhandari*
Hugh Handeyside*
Nathan Freed Wessler*
AMERICAN CIVIL
LIBERTIES UNION
FOUNDATION
125 Broad Street,
18th Floor
New York, NY 10004
(212) 549-2500 (phone)
(212) 549-2583 (fax)
ebhandari@aclu.org
hhandeyside@aclu.org
nwessler@aclu.org

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

**Admitted pro hac vice
Counsel for Plaintiffs*

CERTIFICATE OF SERVICE

I certify that on July 12, 2019, a copy of the foregoing was filed electronically via the Court's ECF system, which effects service upon counsel of record.

/s/ Saira Hussain
Saira Hussain

APPENDIX F

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

No. 17-cv-11730-DJC

GHASSAN ALASAAD et al.,

Plaintiffs,

v.

KEVIN McALEENAN, Acting Secretary of the U.S.
Department of Homeland Security, in his official
capacity et al.,

Defendants.

Hon. DENISE J. CASPER

July 3, 2019

**PLAINTIFFS' RESPONSE TO DEFENDANTS'
STATEMENT OF UNDISPUTED MATERIAL
FACTS AND REPLY IN SUPPORT OF
PLAINTIFFS' STATEMENT OF UNDISPUTED
MATERIAL FACTS**

Pursuant to Fed. R. Civ. P. 56(c) and Local Rule 56.1, Plaintiffs hereby submit their Response to Defendants' Statement of Undisputed Material Facts, ECF No. 98 ("Def. SUMF"), and their Reply in support of Plaintiffs' Statement of Undisputed Material Facts, ECF No. 90-2 ("Pl. SUMF"). Although Plaintiffs dispute Defendants' characterizations of certain

evidence, or dispute that certain facts are material, Plaintiffs do not contend that there are any issues of material fact to be tried.

**PLAINTIFFS' RESPONSE TO DEFENDANTS'
STATEMENT OF UNDISPUTED MATERIAL
FACTS**

**FACTS RELATING TO PLAINTIFF'
CONSTITUTIONAL CLAIMS**

Defendants' Mission Responsibilities:

1. Defendant, Department of Homeland Security ("DHS"), through its components U.S. Customs and Border Protection ("CBP") and U.S. Immigration and Customs Enforcement ("ICE"), has broad powers to prevent the entry of terrorists, and the instruments of terrorism into the United States and to enforce numerous criminal and civil federal laws at the border. *See* 6 U.S.C. § 202, § 211.

Plaintiffs' Response: Defendants' statement is a legal assertion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: Plaintiffs do not dispute that Defendants have the authority to enforce certain laws at the border. Plaintiffs dispute the characterization of Defendants' statutory authority and refer the Court to the relevant statutes themselves. Plaintiffs clarify that the scope of Defendants' statutory authority is circumscribed by the Constitution.

2. CBP's law enforcement mission is primarily interdictive in nature – identifying and mitigating threats to border security and stopping prohibited and

restricted goods and persons from crossing the border, while facilitating and expediting the flow of legitimate travelers and trade. *See* Declaration of Randy J. Howe (“Howe Decl.”) ¶ 7 (Ex. A); 6 U.S.C. § 211.

Plaintiffs’ Response: Defendants’ statement is a legal assertion and/or opinion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: Plaintiffs do not dispute that CBP’s mandate includes preventing prohibited goods and inadmissible persons from entering the United States, while facilitating the flow of legitimate travelers and trade. Plaintiffs dispute Defendants’ characterization of their statutory authority and refer the Court to the relevant statutes themselves. Plaintiffs clarify that the scope of Defendants’ statutory authority is circumscribed by the Constitution.

3. CBP is responsible for enforcing criminal and civil laws and administering comprehensive regulatory schemes relating to immigration, custom, international trade, child pornography, drug smuggling, weapons trafficking, financial crimes as well as national security and terrorism. Howe Decl. ¶ 7. CBP also enforces a host of other laws at the border on behalf of various federal agencies. *Id. See, e.g.*, 31 U.S.C. § 5317; 19 CFR 161.2(a); 19 CFR Part 12.

Plaintiffs’ Response: Defendants’ statement is a legal assertion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: Plaintiffs do not dispute that CBP is responsible for enforcing

certain laws at the border. Plaintiffs dispute the characterization of Defendants' statutory authority and refer the Court to the relevant statutes themselves. Plaintiffs clarify that the scope of Defendants' statutory authority is circumscribed by the Constitution.

4. ICE's Homeland Security Investigations (HSI), is principal investigative arm of DHS and is charged with securing the United States from transnational criminal threats. HSI's mission is to investigate, disrupt, and dismantle terrorist, transnational, and other criminal organizations that threaten or seek to exploit the customs and immigration laws of the United States. HSI enforces a diverse portfolio of federal laws, including all types of cross-border criminal activity. Declaration of David L. Denton ("Denton Decl.") ¶ 5 (Ex. B).

Plaintiffs' Response: Defendants' statement is a legal assertion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: Plaintiffs do not dispute that HSI enforces certain laws at the border. Plaintiffs dispute the characterization of HSI's authority, for which Defendants identify no statutory basis. Plaintiffs clarify that the scope of HSI's authority is circumscribed by the Constitution.

5. To accomplish their mission responsibilities. CBP officers and/or ICE Special Agents may conduct an inspection of the traveler and his or her personal belongings, including any electronic devices. Howe Decl. ¶ 7, 17, 21–23; Denton Decl. ¶¶ 6–7, 11; *see generally* PIA dated August 25, 2009 ("2009 PIA") at

Bates 221–22 (Ex. C.).

Plaintiffs’ Response: Plaintiffs do not dispute that travelers are subject to inspection at the border. Plaintiffs clarify that such inspection, including any search of electronic devices, is subject to statutory and constitutional limits.

Defendants’ Policies:

6. In August 2009, CBP and ICE issued policies on their longstanding authority to search and inspect electronic devices at the international border. *See generally* Border Searches of Electronic Devices, ICE Directive 10044.1 (also known as ICE Directive No. 7-6.1) (Aug. 18, 2009) (Ex. D); Border Search of Electronic Devices Containing Information, CBP Directive No. 3340-049, (Aug. 20, 2009) (Ex. E);

Plaintiffs’ Response: Plaintiffs do not dispute that CBP and ICE issued device-search policies in 2009. Plaintiffs dispute Defendants’ characterization of their border search authority as including warrantless or suspicionless searches of electronic devices, which is additionally a legal assertion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1.

7. In January, 2018, CBP revised its Directive. *See* Border Search of Electronic Devices, CBP Directive No. 3340-049A, (Jan 4, 2018) (“2018 CBP Directive”) (Ex. F). Specifically, 2018 CBP Directive, among other things, (1) clarified the scope of CBP border searches of electronic devices and explicitly stated that measures would be taken to avoid accessing information only stored remotely (*e.g.*, on the “cloud”); (2) distinguished between different types

of searches (basic and advanced); and (3) applied a heightened standard for advanced searches (reasonable suspicion or national security concern). *See id.* ¶ 5.1.

Plaintiffs’ Response: Defendants’ statement with regard to “a heightened standard” lacks support in the cited record materials per Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. Plaintiffs dispute that the CBP 2018 Directive uses the word “heightened” and further dispute, as a legal matter, that the Directive’s “national security concern” standard is a “heightened” standard. Otherwise, no dispute.

8. The updated CBP Directive defines an “advanced search” as any search in which an officer connects external equipment, through a wired or wireless connection, to an electronic device, not merely to gain access to the device, but to review, copy and/or analyze its contents. *Id.* § 5.1.4. A basic search is any border search that is not an advanced search. *Id.* § 5.1.3. The updated Directive further clarified that an advanced search should only be conducted where there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP and ICE or in which there is a national security concern, and requires advance supervisory approval *Id.* § 5.1.4.

Plaintiffs’ Response: Plaintiffs dispute that the CBP 2018 Directive mentions laws enforced or administered by ICE. Otherwise, no dispute.

9. ICE uses the same definitions of basic and advanced searches and only conducts advanced

searches when there is reasonable suspicion. Stipulated Facts ¶¶ 1, 14. (Ex. G); Denton Decl. ¶ 11; HSI Legal Update – Border Search of Electronic Devices, May 11, 2018 at Bates 1266-67.

Plaintiffs’ Response: Plaintiffs do not dispute that ICE uses the same definitions of basic and advanced searches as CBP, and that ICE policy requires that advanced searches be based on reasonable suspicion. To the extent Defendants assert that all advanced searches are, in fact, supported by reasonable suspicion, that assertion lacks support in the cited record materials per Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1; Plaintiffs dispute that assertion and further dispute that it is material.

10. These policies have been carefully crafted to provide the Government, through DHS and its components, with the tools necessary to secure the nation’s border, while simultaneously striving to protect personal privacy. *See* PIA, January 4, 2018 at Bates 0174-0195 (Ex. H).

Plaintiffs’ Response: Defendants’ statement includes legal assertions and/or opinions for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: Plaintiffs dispute that Defendants’ policies permitting warrantless, suspicionless searches of electronic devices are necessary to border security, *see* Pl. SUMF at ¶¶ 92–119, or protective of personal privacy, *see id.* at ¶¶ 63–80.

11. These policies permit CBP Officers and ICE Special Agents to search information contained in electronic devices subject to the guidelines set forth in the policy directives and any other applicable laws. See ICE Directive ¶ 6.1; CBP Directive ¶¶ 4, 5.

Plaintiffs’ Response: No dispute. Plaintiffs clarify that the CBP and ICE policies, and “any other applicable laws,” are subject to constitutional limits.

12. The policies recognize that it is not always possible to complete the search of a traveler’s electronic device while he or she waits at the border. ICE Directive ¶ 6.1; CBP Directive ¶ 5.4. The policies therefore require the searches of detained devices to be completed, in a reasonable time given the facts and circumstances of the particular search. ICE Directive ¶ 8.3(1); CBP Directive ¶ 5.4.

Plaintiffs’ Response: Plaintiffs dispute Defendants’ characterization of what the policies “recognize.” Plaintiffs refer the Court to Pl. SUMF at ¶¶ 11, 12, and 21.

Border Searches:

13. Border inspections are unique and unlike any other law enforcement activity. CBP’s mission to inspect all people and things that cross the border must be balanced with its mission to facilitate the flow of travelers and trade. Howe Decl. ¶ 8; 6 U.S.C. § 211.

Plaintiffs’ Response: Defendants’ statement is a legal assertion and/or opinion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the

extent a response is deemed required: Plaintiffs dispute, as a legal matter, that border inspections are unlike any other law enforcement activity. Plaintiffs further clarify that the referenced statutory authority is circumscribed by the Constitution.

14. Over one million travelers per day go through U.S. ports of entry, and CBP has limited to no advance information about these travelers. The sheer volume of people and merchandise passing through the border each day means CBP has a limited amount of time to determine the specific law enforcement actions appropriate for each encounter. Howe Decl. ¶ 8.

Plaintiffs' Response: Plaintiffs do not dispute Defendants' assessment of the approximate volume of travelers who transit U.S. ports of entry. Plaintiffs dispute Defendants' statement that CBP "has limited to no advance information" about travelers. *See* Exh. 49 (ICE 30(b)(6) depo.) at 159:23– 161:8 (ICE and CBP have access to the Advance Passenger Information System ("APIS"), which provides information about passengers traveling by air prior to their arrival); Exh. 23, ECF No. 91- 22 (Privacy Impact Assessment for the Automated Targeting System ("ATS")) at Bates 998 (ATS ingests data from the APIS); Pl. SUMF at ¶¶ 28, 36–44 (ATS generates "lookouts" that prompt referrals of travelers to secondary inspection). Plaintiffs do not dispute that CBP has a limited amount of time to undertake any law enforcement actions during encounters with travelers at the border.

15. CBP officers evaluate the totality of the circumstances for each encounter at the border and will consider every piece of relevant information available to determine if the person and goods are admissible into the United States, if there is a violation of any of the laws CBP enforces, or if there is a threat to border security. Howe Decl. ¶¶ 10, 14-16. The ability to engage in these actions and the discretion to determine – based on the totality of the circumstances – which actions are appropriate in a given inspection is crucial to CBP’s ability to secure the border and identify and interdict threats to national security. *Id.* ¶ 16.

Plaintiffs’ Response: Plaintiffs do not dispute that CBP’s policy is for officers to evaluate the totality of the circumstances during encounters at the border, and to consider all relevant information available in determining whether a person or goods are admissible into the United States, if there is a violation of the any of the laws CBP enforces, or if there is a threat to border security. To the extent that Defendants assert CBP officers evaluate the totality of the circumstances in every instance, that assertion lacks support in the record per Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1; Plaintiffs dispute that assertion and further dispute that it is material. The second sentence is a statement of opinion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: Defendants’ reference to “these actions” is

vague and ambiguous. Plaintiffs do not dispute that CBP officers exercise some discretion in determining which actions to take during a given inspection. To the extent the “actions” include searches of electronic devices, Plaintiffs dispute that such searches are “crucial to CBP’s ability to secure the border and identify and interdict threats to national security.” See Pl. SUMF at ¶¶ 92–98 (non-prevalence of digital contraband at the border); 99–102 (lack of evidence that warrantless, suspicionless device searches are effective); 103–119 (feasibility of obtaining warrants and/or applying probable cause and reasonable suspicion standards).

16. TECS is CBP’s principal law enforcement and anti-terrorism database system used at the border to assist with inspections and determinations regarding admissibility of arriving persons. Howe Decl. ¶ 9. TECS includes law enforcement “lookouts” and other records entered by CBP and other law enforcement agencies regarding persons of interest. *Id.* TECS also includes law enforcement records documenting certain inspections conducted by CBP at the border, including border searches of electronic devices. *Id.*

Plaintiffs’ Response: No dispute.

17. CBP’s documentation of its inspections are official government records made by the agency to evidence the decisions made and activities undertaken by CBP during the course of the encounter. Howe Decl. ¶ 9.

Plaintiffs’ Response: Defendants’ statement is a legal assertion for which no response is

required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: no dispute. Plaintiffs clarify that such records, including TECS records, may be subject to expungement if collected in violation of the Constitution.

18. Upon arrival at a port of entry, at the primary point of inspection, CBP Officers inspect travelers' documentation (e.g., passport, customs declaration), ask questions regarding their travel and search CBP systems for relevant information. Howe Decl. ¶12. At primary, a CBP Officer may conduct limited queries of information maintained in TECS. *Id.* The information available to an officer at primary does not generally include information relating to past border searches of electronic devices. *Id.*

Plaintiffs' Response: No dispute.

19. If CBP has advance information about travelers or merchandise, CBP compares the advance information against law enforcement and intelligence information and conducts risk assessments to identify travelers or merchandise that warrant additional scrutiny, and a "lookout" can be placed in the TECs system to advise officers to perform additional scrutiny. Howe Decl. ¶ 11.

Plaintiffs' Response: To the extent Defendants assert that travelers or merchandise that are the subjects of "lookouts" actually warrant additional scrutiny in all instances, that assertion lacks support in the record per Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1; Plaintiffs dispute that

assertion and further dispute that it is material. Otherwise, no dispute.

20. CBP has little to no advance travel information about individuals traveling across land ports of entry. Howe Decl. ¶ 33.

Plaintiffs’ Response: No dispute.

21. The vast majority of border searches of electronic devices are basic searches that may be as short as a matter of minutes and that may involve briefly scrolling through the device. Howe Decl. ¶ 31. In many instances, a brief, basic search is sufficient to alleviate – or heighten – concerns presented during a border inspection. *Id.*

Plaintiffs’ Response: Plaintiffs refer the Court to Pl. SUMF at ¶¶ 53 and 54, which set forth the precise numbers of basic and advanced device searches CBP conducted in fiscal years 2012 through 2017. Plaintiffs clarify that ICE does not maintain records of the number of basic searches it conducts, *see* Pl. SUMF at ¶ 56, and therefore cannot identify what percentage of the overall number of device searches it conducts are basic searches. Plaintiffs do not dispute that basic searches of electronic devices may be as short as “a matter of minutes” but Plaintiffs clarify that Defendants place no limit on how long a basic search may take. *See* Exh. 50 (CBP 30(b)(6) depo.) at 140:16–18 (Q: “Are there limits on how long a basic search can take?” A: “Not until we’re satisfied.”). Defendants’ reference to “many instances” is vague and ambiguous. Plaintiffs do not dispute that a basic search

could alleviate or heighten concerns during a border inspection.

22. Given the volume of travelers that CBP processes, and in order to ensure efficiency, if based on his or her extensive training and experience, a CBP officer determines that additional scrutiny beyond the brief initial encounter is warranted, the traveler will be referred for a continuation of their inspection, often referred to as “secondary” or “secondary inspection.” Howe Decl. ¶ 13. A secondary inspection is a continuation of the border inspection and an officer may refer any traveler to secondary inspection. *Id.*

Plaintiffs’ Response: Plaintiffs dispute Defendants’ characterization of “extensive training and experience” as applying generally to all CBP officers or in all circumstances. Otherwise, no dispute.

23. At secondary, the CBP officer may run law enforcement queries through TECS and other CBP systems. Howe Dec. ¶ 13. The information available to officers at secondary includes the same types of information available at primary, but may also include additional records relating to prior encounters between the traveler and CBP. Howe Decl. ¶13.

Plaintiffs’ Response: No dispute.

24. CBP shares its border search authority with ICE whose HSI Special Agents are also designated as customs officers and immigration officers, in addition to being criminal investigators. Where circumstances warrant, CBP Officers may notify ICE HSI of a matter encountered during the course of a border inspection and ICE HSI agents may engage in additional follow-up investigation, particularly where the matter may

be a candidate for criminal prosecution Howe Decl. ¶ 18; Denton Decl. ¶ 12.

Plaintiffs’ Response: Defendants’ statement regarding ICE’s border search authority is a legal assertion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: Plaintiffs do not dispute that ICE designates HSI agents as customs officers, immigration officers, and “criminal investigators.” Plaintiffs also do not dispute that CBP officers sometimes notify HSI of a matter encountered during the course of a border inspection, and that HSI agents then engage in follow-up investigation. To the extent Defendants assert that “circumstances warrant” such notification and/or follow-up investigation in all instances, that assertion lacks support in the record per Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1; Plaintiffs dispute that assertion and further dispute that it is material.

25. HSI does not undertake border searches to uncover evidence of crimes that lack a nexus to the border. Denton Decl. ¶ 10. However, during a border search HSI Special Agents may encounter evidence of crimes that have no border nexus and may share the information with the agency responsible for enforcing or administering the applicable law or, as federal law enforcement officers generally empowered to enforce federal criminal law, act on it themselves. *Id.*

Plaintiffs’ Response: Plaintiffs dispute that “HSI does not undertake border searches to uncover evidence of crimes that lack a nexus to

the border.” See Def. Resp. to Pl. SUMF, ECF No. 98 at ¶ 84 (ICE conducts warrantless or suspicionless border searches of electronic devices to find evidence of law violations unrelated to the border when it is “also investigating that individual for violation of a cross-border crime within the jurisdiction of ICE”). Plaintiffs do not dispute that HSI agents sometimes share information with the agency responsible for enforcing or administering the applicable law, or that HSI agents sometimes act on such information themselves. Plaintiffs dispute Defendants’ characterization of HSI agents as “officers generally empowered to enforce federal criminal law.”

26. Prior to conducting a border search, HSI Special Agents can review information on a traveler contained in various government systems, including CBP’s record systems and in ICE’s Investigative Case Management System (ICM). Denton Decl. ¶ 14.

Plaintiffs’ Response: No dispute.

27. ICM is a system that enables ICE personnel to create an electronic case file that organizes and links all records and documents associated with an investigation, so they are easily accessible from a single location and enables personnel to link records to multiple investigations. Denton Decl. ¶ 14.

Plaintiffs’ Response: No dispute.

28. When a border search is conducted, HSI Special Agents must record the occurrence of a search in ICE’s Investigation Case Management System (ICM). Denton Decl. ¶15. Special Agents can also

record in ICM their impressions of the search or notable observations. *Id.*

Plaintiffs' Response: No dispute.

29. ICM does not contain the forensic copies of the data on any electronic device, which are stored separately. Denton Decl. ¶ 15. ICM only contains the descriptions that a Special Agent may make of what is observed during a search. *Id.* These federal records are maintained in accordance with section 8.5(1)(b) of ICE Directive 10044.1. *Id.*

Plaintiffs' Response: No dispute as to the first and second sentences. The third sentence is a legal assertion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: To the extent Defendants assert that ICM records are maintained in accordance with section 8.5(1)(b) of ICE Directive 10044.1 in all instances, that assertion lacks support in the record per Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1; Plaintiffs dispute that assertion and further dispute that it is material. Plaintiffs further clarify that such records may be subject to expungement if collected in violation of the Constitution.

30. In FY 2017, CBP conducted 30,524 border searches of electronic devices and processed more than 397 million arriving international travelers; only approximately 0.007% of arriving travelers had their devices searched. Less than 3,500 of those searches were advanced searches. *See Stipulated Facts 13; Response to Interrog. 6. (Ex. I).* In that same year, ICE

conducted only 681 advanced searches. Stipulated Facts 15.

Plaintiffs' Response: No dispute.

Warrantless Border Searches of Electronic Devices
Support Defendants' Mission

31. All persons, conveyances, cargo, baggage, personal effects and merchandise of every description may be subject to a border inspection, inbound or outbound. Howe Decl. ¶ 21. This may include things as varied as a shipping container, a mobile home, a suitcase, or a purse, along with any items these things might contain. *Id.*

Plaintiffs' Response: No dispute. Plaintiffs clarify that border inspections are subject to statutory and constitutional limits.

32. As international travelers carry more electronic devices, there is a greater likelihood that information that was previously maintained in hard copy form, and easily accessible to CBP Officers, is now maintained electronically. Howe Decl. ¶ 26.

Plaintiffs' Response: Defendants' statement lacks foundation and is an opinion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: Plaintiffs do not dispute that some information previously maintained in hard copy form is now maintained electronically. Plaintiffs dispute Defendants' unsupported assertions regarding the "likelihood" that information that was previously maintained in hard copy form is now maintained electronically, and the ease with

which CBP officers previously accessed information in hard copy form, which lack support in the record per Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. Plaintiffs refer the Court to Pl. SUMF at ¶¶ 63–64 (volume and range of information stored in electronic devices).

33. Electronic devices themselves are merchandise and can contain both merchandise and evidence relating to merchandise. There is a myriad of electronic devices, such as computers, phones, tablets, flash drives, and SD Cards, which can all be encountered at the border. Denton Decl. ¶ 7; Howe Decl. ¶¶ 23, 25.

Plaintiffs’ Response: The first sentence is a legal assertion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: Plaintiffs dispute, as a legal matter, that all electronic devices themselves are merchandise, and further dispute that this is a material fact. Defendants’ statement that electronic devices can contain merchandise is vague and ambiguous. Plaintiffs do not dispute that electronic devices can contain evidence related to merchandise. No dispute as to the second sentence.

34. Electronic border device searches advance the Defendants interest in stopping contraband because electronic devices can contain illegal goods just as easily as any other container. *See* Howe Decl. ¶¶ 23, 39; Denton Decl. ¶¶ 7-8, 16.

Plaintiffs’ Response: Defendants’ statement

is a legal assertion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: Plaintiffs do not dispute that electronic devices can contain illegal content in the form of digital data but do dispute that such illegal content is the equivalent of “illegal goods” stored in a physical container. Plaintiffs dispute, as a legal matter, that warrantless or suspicionless border searches of electronic devices sufficiently advance Defendants’ interests or outweigh the extraordinary privacy interests travelers have in their devices. *See* Pl. SUMF at ¶¶ 63–76 (sensitivity of content and invasiveness of searches); 92–98 (non-prevalence of digital contraband at the border); 99–102 (lack of evidence that warrantless, suspicionless device searches are effective); 103–119 (feasibility of obtaining warrants and/or applying probable cause and reasonable suspicion standards).

35. Electronic devices can contain many types of “digital contraband” such as child pornography, classified information, and counterfeit media. *See* Howe Decl. ¶ 23.

Plaintiffs’ Response: Plaintiffs dispute Defendants’ assertion that electronic devices can contain “many” types of digital contraband, which lacks foundation and is not supported by the record. Plaintiffs do not dispute that electronic devices can contain more than one type of digital contraband. Plaintiffs note that Defendants’ declarant, when testifying as a Rule 30(b)(6) witness on behalf of Defendant

CBP, did not identify types of digital contraband other than child pornography. Exh. 13, ECF No. 91-12 (CBP 30(b)(6) depo.) at 62:8–66:15.

36. Electronic devices can also contain evidence of contraband, such as child pornography or items that violate intellectual property rights; classified information; export controlled material, drug trafficking, firearm smuggling, and export control violations. Howe Decl. ¶¶ 23-24, 28, 30; Denton Decl. ¶¶ 24-27.

Plaintiffs’ Response: Plaintiffs dispute that Defendants’ statement accurately characterizes the cited material. The Howe Declaration states, “Electronic devices can also contain records which constitute evidence of a crime or other legal violation,” which Plaintiffs do not dispute. Exh. A, ECF No. 98-1 (Howe Decl.) at ¶ 23.

37. Defendants’ 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. Howe Decl. ¶¶ 27-30; Denton Decl. ¶¶ 16, 24-27.

Plaintiffs’ Response: Plaintiffs dispute Defendants’ statement because it lacks foundation per Federal Rule of Civil Procedure 56(c)(2)/Local Rule 56.1. To the extent a response is deemed required: Defendants’ reference to “threats to national security” and “information pertaining to terrorism” are vague and ambiguous. Plaintiffs do not dispute that

border searches of electronic devices have uncovered digital contraband. Plaintiffs refer the Court to Pl. SUMF at ¶¶ 92–98 (non-prevalence of digital contraband at the border); 99–102 (lack of evidence that warrantless, suspicionless device searches are effective).

38. There have been numerous instances where CBP conducted searches without any advance information or suspicion and found evidence that revealed threats to national and/or border security. Howe Decl. ¶ 28.

Plaintiffs’ Response: Plaintiffs do not dispute that the Howe Declaration provides this assertion. Defendants’ reference to “numerous instances” and “threats to national and/or border security” are vague and ambiguous. Defendants’ reference to “evidence” in the context of “threats to national and/or border security”—*i.e.*, absent an indication that a traveler was carrying contraband or engaged in illegal activity—is vague and ambiguous. Plaintiffs refer the Court to Pl. SUMF at ¶¶ 92–98 (non-prevalence of digital contraband at the border); 99–102 (lack of evidence that warrantless, suspicionless device searches are effective).

39. There have been numerous instances where CBP conducted searches without any advance information or suspicion and found evidence that contradicted an individual’s state purpose for travel to the United States. Howe Decl. ¶ 29.

Plaintiffs’ Response: Defendants’ statement lacks foundation. Defendants’ reference to

“numerous instances” is vague and ambiguous. Defendants’ reference to “evidence” in the context of “an individual’s state [sic] purpose for travel to the United States” is vague and ambiguous. Plaintiffs dispute that Defendants’ statement accurately characterizes the cited material. Paragraph 29 of the Howe Declaration states, “I am also personally familiar with situations in which CBP Officers exercised their discretion to refer an individual for additional scrutiny and the resulting search of the subject’s electronic device revealed information that clearly contradicted the individual’s stated purpose for travel to the United States,” which Plaintiffs do not dispute, but Plaintiffs do dispute that this testimony supports Defendants’ statement of fact that the searches were done “without any advance information or suspicion.” Exh. A, ECF No. 98-1 (Howe Decl.) at ¶ 29. Plaintiffs refer the Court to Pl. SUMF at ¶¶ 2 (admissibility of U.S. citizens and lawful permanent residents); 99-102 (lack of evidence that warrantless, suspicionless device searches are effective).

40. There have been numerous instances where CBP conducted searches without any advance information or suspicion and found evidence that could be used to support a criminal prosecution, such as child pornography, narcotics. Howe Decl. ¶ 30.

Plaintiffs’ Response: Defendants’ statement lacks foundation. Defendants’ reference to “numerous instances” is vague and ambiguous. Plaintiffs dispute that Defendants’ statement accurately characterizes the cited material.

Paragraph 30 of the Howe Declaration states, “I am aware of instances where border searches of electronic devices have revealed information that was used to support a criminal prosecution,” which Plaintiffs do not dispute, but Plaintiffs do dispute that this testimony supports Defendants’ statement of fact that the searches were done “without any advance information or suspicion.” Exh. A, ECF No. 98-1 (Howe Decl.) at ¶ 30.

41. Electronic devices can also contain information that facilitates the execution of the non-criminal aspects of CBP’s mission, which includes the enforcement of civil and administrative legal requirements. Howe Decl. ¶ 30.

Plaintiffs’ Response: Defendants’ reference to “information that facilitates the execution of the non-criminal aspects of CBP’s mission” is vague and ambiguous. Plaintiffs do not dispute that electronic device searches have, in some instances, revealed information relevant to the enforcement of civil and administrative legal requirements.

42. Border search authority is a crucial tool and requiring a warrant for all border searches of electronic devices would significantly impede CBP’s and ICE’s missions. Howe Decl. ¶¶ 26, 32; Denton Decl. ¶¶ 18, 23-27.

Plaintiffs’ Response: Defendants’ statement lacks foundation and is an opinion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: The

phrase “significantly impede” is vague and ambiguous. Plaintiffs dispute that warrantless or suspicionless searches of electronic devices are a “crucial tool” or that requiring a warrant for such searches would “significantly impede CBP’s and ICE’s missions.” *See* Pl. SUMF at ¶¶ 92–98 (non-prevalence of digital contraband at the border); 99–102 (lack of evidence that warrantless, suspicionless device searches are effective); 103–119 (feasibility of obtaining warrants and/or applying probable cause and reasonable suspicion standards).

43. Due to the differences between a typical law enforcement encounter and the border, it is highly unlikely that probable cause exists in the border context. First, a border search is generally not a search where the places and things to be searched can be particularly described in advance, as required in a warrant, but is a search of the individual and her belongings as she chooses to present them at the border. Second, the things to be searched at the border are not those identified, described, and targeted by the government, but whatever the traveler chooses to carry with her across the border between nations. Denton Decl ¶ 22; Howe Decl. ¶¶ 33-34.

Plaintiffs’ Response: Plaintiffs dispute Defendants’ statement because it lacks foundation per Federal Rule of Civil Procedure 56(c)(2)/Local Rule 56.1 and is an opinion for which no response is required under Federal Rule of Civil Procedure 56(c)(1) and/or Local Rule 56.1. To the extent a response is deemed required: The phrase “highly unlikely” is vague and ambiguous. Plaintiffs note that the CBP

2018 Directive contemplates probable cause to seize and retain an electronic device based on “facts and circumstances” other than information derived from the device itself. Exh. 19, ECF No. 91-18 (CBP 2018 Directive) at § 5.5.1.1, Bates 121. Finally, Defendants’ statement is immaterial, in that it assumes that a warrant and/or probable cause must be obtained prior to a traveler’s arrival at the border. Plaintiffs’ claims entail no such requirement. *See* Am. Compl., ECF No. 7 at ¶¶ 169, 171, 173.

44. A warrant necessarily requires advance information to support the probable cause determination, requires the time and deliberateness associated with review by a neutral magistrate, and requires the identification of a specific person or thing to be searched and the particular crime that is implicated. In a border environment, such advance information necessary to support probable cause for search is often minimal. *Howe Decl.* ¶ 34.

Plaintiffs’ Response: Plaintiffs dispute Defendants’ statement that “a warrant necessarily requires advance information;” that statement lacks foundation and is immaterial, in that it assumes that a warrant and/or probable cause must be obtained prior to a traveler’s arrival at the border. Plaintiffs’ claims entail no such requirement. *See* Am. Compl., ECF No. 7 at ¶¶ 169, 171, 173. *See also* Pl. SUMF at ¶¶ 103–119 (feasibility of obtaining warrants and/or applying probable cause and reasonable suspicion standards).

45. A warrant requirement is impractical, if not impossible, for the government to obtain because the what, where, how, and when she presents herself and her possessions at the border is generally not knowable to the government in advance. Denton Decl ¶ 22; Howe Decl. ¶¶ 34.

Plaintiffs’ Response: Defendants’ statement lacks foundation and is an opinion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: The phrase “impractical, if not impossible” is vague and ambiguous. Plaintiffs dispute Defendants’ statement and further dispute that it is material, in that it assumes that the basis for a warrant must be “knowable to the government in advance.” Plaintiffs’ claims entail no such requirement. *See* Am. Compl., ECF No. 7, at ¶¶ 169, 171, 173. *See also* Pl. SUMF at ¶¶ 103–119 (feasibility of obtaining warrants and/or applying probable cause and reasonable suspicion standards).

46. Requiring a warrant for electronic devices at the border would have serious consequences for border security by creating a category of, and a container for, merchandise immune from border search. Such an obvious loophole in the ability of the United States to patrol its borders would create a safe-haven for contraband and evidence and inevitably result in exploitation by criminals, terrorists, and transnational criminal organizations to smuggle merchandise, contraband, and evidence of criminal conspiracies into and out of the United States. Denton Decl. ¶¶ 18, 23; Howe Decl. ¶ 32, 35.

Plaintiffs’ Response: Defendants’ statement is speculative and is an opinion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: The phrases “serious consequences,” “obvious loophole,” and “safe-haven” are vague and ambiguous. Plaintiffs dispute Defendants’ statement, which lacks foundation, in that it wrongly assumes that digital contraband must and will transit borders via travelers’ electronic devices. *See* Pl. SUMF at ¶¶ 95–98 (transmission of digital contraband via the internet).

47. A warrant requirement would obviate the deterrent effect of border searches when it comes to electronic devices and incentivize criminals to store contraband or other evidence of illegal goods on their electronic devices. *See* Howe Decl. ¶¶ 38, 43; Denton Decl. ¶¶ 18, 23.

Plaintiffs’ Response: Defendants’ statement is speculative and an opinion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: Plaintiffs dispute Defendants’ statement, which lacks foundation in assuming that Defendants’ current policies create a meaningful deterrent effect, and that digital contraband must and will transit borders via travelers’ electronic devices. *See* Pl. SUMF at ¶¶ 95–98 (transmission of digital contraband via the internet).

48. A warrant requirement would impose entirely unknown logistical and resource requirements on Defendants. Howe Decl. ¶¶ 34, 36; Denton Decl. ¶¶ 19-22.

Plaintiffs’ Response: Defendants’ statement is speculative and an opinion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: Plaintiffs dispute that Defendants’ statement accurately characterizes the cited declarations. Plaintiffs further dispute that a warrant requirement would impose “entirely unknown” requirements. Plaintiffs refer the Court to Pl. SUMF at ¶¶ 103–115 (feasibility of obtaining warrants in similar contexts).

49. A warrant requirement for border searches of electronic devices would likely impede CBP’s ability to expeditiously complete certain border inspections; would likely prevent CBP from detecting electronic contraband; and would deprive the federal government of crucial information, including terrorism related information, that informs admissibility determinations relating to both people and goods. Howe Decl. ¶¶ 32, 36-38.

Plaintiffs’ Response: Defendants’ statement is speculative and is an opinion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: The phrases “crucial information” and “terrorism related information” are vague and ambiguous. Plaintiffs dispute Defendants’ statement, which lacks foundation. See Pl. SUMF ¶¶ 95–

98 (transmission of digital contraband via the internet); 99–102 (lack of evidence that warrantless, suspicionless device searches are effective); 103–119 (feasibility of obtaining warrants and/or applying probable cause and reasonable suspicion standards).

50. A warrant requirement would threaten the security of this country. Defendants have on numerous occasions interdicted contraband and criminals through use of device border searches, and in most, if not all, of these instances the Government did not have a warrant or probable cause to conduct the search at issue. *See* Howe Decl. ¶ 27-30; Denton Decl. ¶¶ 24-27.

Plaintiffs’ Response: Defendants’ first sentence is speculative and is an opinion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: The phrase “threaten the security of this country” is vague and ambiguous. Defendants’ second sentence lacks foundation, and Plaintiffs dispute that it accurately characterizes the cited declarations, which neither set forth “numerous occasions” in which Defendants interdicted contraband nor identify data indicating that the government lacked probable cause in “most, if not all” such instances. *See* Pl. SUMF at ¶¶ 92–98 (non-prevalence of digital contraband at the border); 99–102 (lack of evidence that warrantless, suspicionless device searches are effective); 103–119 (feasibility of obtaining warrants

and/or applying probable cause and reasonable suspicion standards).

FACTS RELATING TO INDIVIDUAL PLAINTIFFS:

51. Out of the eleven Plaintiffs, seven have had their electronic devices searched at the border only once (Plaintiffs Ghassan Alasaad, Allababidi, Bikkannavar, Gach, Shilby, Wright, and Zorri). *See* Pls. SUMF ¶¶ 120-149 (ECF 90-2).

Plaintiffs' Response: No dispute.

52. Four have had their electronic devices searched at the border more than once (Plaintiffs Merchant, Nadia Alasaad, Dupin and Kushkush). *See* Pls. SUMF ¶¶ 121, 123, 129, 130, 134, 135, 137, 140, 141, 142 (ECF 90-2).

Plaintiffs' Response: No dispute.

53. Except for Plaintiff Merchant, none of the Plaintiffs have had their electronic devices searched since August 2017. *See* Pls. SUMF ¶¶ 120-149. (ECF 90-2)

Plaintiffs' Response: No dispute.

54. Plaintiff Merchant did have her electronic device manually searched in September, 2018 but she has travelled internationally at least five times since her most recent search and has not been searched during any of those trips. *See* Ex. J, Merchant Resp. to Interrogs. 1, 4; Merchant Suppl. Resp. to Interrogs. 1, 4, 7.

Plaintiffs' Response: Plaintiffs do not dispute that Plaintiff Merchant has not been subjected to a search of her electronic devices by

Defendants during her international trips subsequent to September 2018. *See* Exh. J, ECF No. 98-10 (Merchant responses to Interrogatories 1, 4 and Merchant supplemental responses to Interrogatories 1, 4, and 7).

55. Defendants deleted all copies of Plaintiff Wright's data. Declaration of Jenny Tsang, (Ex. L).

Plaintiffs' Response: No dispute.

PLAINTIFFS' REPLY IN SUPPORT OF PLAINTIFFS' STATEMENT OF UNDISPUTED MATERIAL FACTS

I. Defendants' Policies and Practices on Border Searches and Confiscations of Travelers' Electronic Devices

A. CBP Screening

1. U.S. Customs and Border Protection ("CBP") officers conduct primary inspections of every person who crosses the border into the United States at a port of entry. Exh. 13 (CBP 30(b)(6) depo.) at 85:3–12.

Defendants' Response: Dispute the characterization as a "primary" inspection here, but admit that CBP officers conduct inspections of every person who crosses the border into the United States at a port of entry. *Id.*

Plaintiffs' Reply: Defendants do not raise a genuine dispute. Plaintiffs' reference to "primary" refers to the first point of contact for every traveler.

2. During primary inspections, CBP officers must determine whether a traveler seeking entry is admissible to the United States. U.S. citizens are by definition admissible. Lawful permanent residents, with some exceptions, are also by definition admissible. Officers must also determine whether the traveler is carrying goods subject to customs rules, such as prohibited contraband. Exh. 13 (CBP 30(b)(6) depo.) at 35:2–5, 80:4–8, 85:3–12 & errata pages.

Defendants’ Response: Dispute that this determination only occurs during “primary” inspection and also dispute their characterization of the term “lawful permanent resident.” Admit that U.S. citizens are by definition admissible once they establish their identity and citizenship to the satisfaction of the inspecting officer. *Id.* at 35:4-5. Aliens lawfully admitted for permanent residence in the United States are also not regarded as seeking admission for purposes of immigration laws unless certain criteria apply. *See* 8 U.S.C. §1101(a)(13)(C). Further dispute the characterization that Officers are determining “whether the traveler is carrying goods subject to customs rules, such as prohibited contraband;” all goods crossing the border are subject to inspection by customs officers. *See* 19 U.S.C. § 1401(c); *see also* Exh. 13 (CBP 30(b)(6) depo.) at 35:15-36::17

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. Plaintiffs do not dispute Defendants’ characterizations of “primary” inspection and “lawful permanent resident.” Defendants’ statement that “all goods crossing

the border are subject to inspection by customs officers” is a legal assertion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent that a response is deemed required: no dispute. Plaintiffs clarify that Defendants’ statutory authority is subject to constitutional limits.

3. If a CBP officer at primary inspection decides that a traveler warrants further screening, the officer will refer the traveler to secondary inspection. Exh. 13 (CBP 30(b)(6) depo.) at 87:6–18.

Defendant’s Response: Dispute that this statement correctly characterizes the cited deposition testimony. Admit that a CBP officer at primary inspection may refer a traveler for additional scrutiny if they require further time for processing.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. The CBP deposition testimony states that if the primary inspection officer is “unable to [make that quick and efficient determination] in a reasonable amount of time,” CBP has “secondary inspection.” Exh. 13, ECF No. 91-12 (CBP 30(b)(6) depo.) at 87:9–18.

4. Some travelers are randomly selected for referral to secondary inspection. Exh. 18 (CBP Briefing for Senate Committee) at Bates 282.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

5. During secondary inspections, when deciding whether to search a traveler’s device,

CBP officers consider past border searches of electronic devices. Exh. 13 (CBP 30(b)(6) depo.) at 122:4–13.

Defendants’ Response: Dispute that this statement correctly characterizes the cited deposition testimony which makes clear that a CBP officer considers a number of factors in deciding whether to search a traveler’s device which may include past searches. *Id.* at 122:4-20.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. The CBP deposition testimony states that “[t]he officer has to rely on their training, experience, and the totality of the circumstances they have before them,” which also includes information about past border searches of electronic devices. *See* Exh. 13, ECF No. 91-12 (CBP 30(b)(6) depo.) at 122:4–20.

B. The CBP Policy

6. CBP’s border searches and confiscations of electronic devices are governed by CBP Directive No. 3340–049A, dated January 4, 2018 (the “CBP Policy”). Exh. 19 (CBP 2018 Directive) at § 11, Bates 124.

Defendants’ Response: Dispute the characterization of the cited policy. Admit that CBP Directive No. 3340–049A, dated January 4, 2018 (the “CBP Policy”) provides guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in electronic devices.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. Plaintiffs define “confiscations” as seizures of travelers’ electronic devices after a traveler has left the border.

7. In an “advanced” or “forensic” search, an officer connects external equipment to a traveler’s electronic device, with a wired or wireless connection, in order to access, review, copy, and/or analyze the contents of the device. Exh. 46 (Stipulations) at ¶ 1; Exh. 19 (CBP 2018 Directive) at § 5.1.4, Bates 117; Exh. 20 (ICE Broadcast) at Bates 1266; Exh. 14 (ICE 30(b)(6) depo.) at 54:14–23.

Defendants’ Response: Dispute that plaintiffs correctly characterized the referenced Stipulation and refer the Court to the Stipulation and CBP 2018 Directive for an accurate statement. Do not dispute that an advanced search is defined in both the Stipulation and CBP 2018 Directive 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.”

Plaintiffs’ Reply: Defendants do not raise a genuine dispute.

8. In a “basic” or “manual” search, an officer reviews the content of a traveler’s electronic device without using external equipment. Exh. 19 (CBP 2018 Directive) at § 5.1.3, Bates 116; Exh. 14 (ICE 30(b)(6) depo.) at 54:14–55:3.

Defendants’ Response: Dispute that the CBP

2018 Directive uses the term “manual” to describe a search. Exh 19 at § 5.1.3 (describing a basic search). Do not dispute that the term “manual” is sometimes used to describe a basic search.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute.

9. The CBP Policy allows advanced searches of electronic devices based on either “reasonable suspicion of activity in violation of the laws enforced or administered by CBP” or a “national security concern.” Exh. 19 (CBP 2018 Directive) at § 5.1.4, Bates 117.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

10. The CBP Policy allows basic searches of electronic devices without any suspicion. Exh. 19 (CBP 2018 Directive) at § 5.1.3, Bates 116.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

11. The CBP Policy allows officers to retain travelers’ electronic devices for on-site or off-site searches, which “ordinarily” should not exceed five days, but can be prolonged with supervisory approval based on “extenuating circumstances.” Exh. 19 (CBP 2018 Directive) at §§ 5.4.1–5.4.1.1, Bates 119.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

12. The CBP Policy places no ultimate limit on how long a device can be kept for search. Exh. 13 (CBP

30(b)(6) depo.) at 223:21–224:7.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

13. The CBP Policy permits CBP to retain information from a traveler’s device that is related to “immigration, customs, and other enforcement matters,” even if there is no probable cause to suspect a violation of law. Exh. 19 (CBP 2018 Directive) at § 5.5.1.2, Bates 121.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

14. The CBP Policy permits officers to share information retained from electronic devices with federal, state, local, and foreign law enforcement agencies. Exh. 19 (CBP 2018 Directive) at § 5.5.1.3, Bates 122.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

15. CBP does not know how long other government entities keep the information they receive from CBP’s border searches of electronic devices. Exh. 13 (CBP 30(b)(6) depo.) at 200:2–12.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

16. CBP does not monitor whether other government entities impermissibly retain the information CBP shares from border searches of electronic devices. Exh. 13 (CBP 30(b)(6) depo.) at 203:7–204:3.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

C. The ICE Policy

17. U.S. Immigration and Customs Enforcement's ("ICE") border searches and confiscations of electronic devices are governed by ICE Directive No. 7–6.1 (also known as ICE Policy 10044.1), dated August 18, 2009, as superseded in part by an ICE/Homeland Security Investigations ("HSI") Broadcast, dated May 11, 2018 (collectively, the "ICE Policy"). Exh. 21 (ICE 2009 Directive) at Bates 260–69; Exh. 20 (ICE Broadcast) at Bates 1266–67; Exh. 14 (ICE 30(b)(6) depo.) at 149:10–20, 187:21–188:2.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

18. The ICE Policy allows advanced searches of electronic devices with reasonable suspicion. Exh. 20 (ICE Broadcast) at Bates 1266–67.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

19. The ICE Policy allows basic or manual searches of electronic devices without any suspicion. Exh. 21 (ICE 2009 Directive) at § 6.1, Bates 261.

Defendants' Response: Dispute that the ICE policy uses the term "manual" to describe a search. The correct term is basic. *Id.*

Plaintiffs' Reply: Defendants do not raise a genuine dispute.

20. When CBP turns an electronic device over to

ICE for a search, ICE policy applies. Exh. 21 (ICE 2009 Directive) at § 6.2, Bates 261; Exh. 19 (CBP 2018 Directive) at § 2.7, Bates 114.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

21. The ICE Policy allows agents to take and retain travelers’ electronic devices for on-site or off-site searches. Exh. 21 (ICE 2009 Directive) at § 8.1(4), Bates 263. The ICE Policy states that such searches should “generally” be completed within 30 days, but can be prolonged with supervisory approval. *Id.* at § 8.3(1), Bates 263–64.

Defendants’ Response: Dispute plaintiffs’ characterization of the ICE policy which requires agents “to complete the search of detained electronic devices, or copies of information therefrom, in a reasonable time give the facts and circumstances of the particular search” and refer the Court to the policy (Exh 21 §8.3) for an accurate statement.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. The ICE 2009 Directive states: “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 . . .* Any detention exceeding 30 calendar days must be approved by a Group Supervisor or equivalent . . .” Exh. 21, ECF No. 91-20 (ICE 2009 Directive) at § 8.3(1), Bates

263–64 (emphases added).

22. The ICE Policy permits ICE to retain information from travelers’ devices that are “relevant to immigration, customs, and other law enforcement matters.” Exh. 21 (ICE 2009 Directive) at § 8.5(1)(b), Bates 266.

Defendants’ Response: No dispute that the ICE policy permits retention of information to the extent authorized by law and if retention is consistent with the privacy and data protection policies of the system in which the information is retained. *Id.*

Plaintiffs’ Reply: No dispute. The ICE 2009 Directive states: “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.” Exh. 21, ECF No. 91-20 (ICE 2009 Directive) at § 8.5(1)(b), Bates 266.

23. The ICE Policy states that copies of information from travelers’ devices that are “determined to be of no relevance to ICE” must be destroyed, and the destruction must be documented. Exh. 21 (ICE 2009 Directive) at § 8.5(1)(e), Bates 267.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

24. The ICE Policy permits ICE to share information retained from electronic devices with federal, state, local, and foreign law enforcement

agencies. Exh. 21 (ICE 2009 Directive) at § 8.5(1)(c), Bates 266.

Defendants’ Response: No dispute that the ICE policy allows sharing of information in accordance with applicable law and policies.

Plaintiffs’ Reply: No dispute. The ICE 2009 Directive states: “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, or foreign law enforcement agencies in accordance with applicable law and policy.” Exh. 21, ECF No. 91-20 (ICE 2009 Directive) at § 8.5(1)(c), Bates 266.

A. Border Screening Databases

1. CBP’s TECS

25. TECS is CBP’s main database. Exh. 13 (CBP 30(b)(6) depo.) at 46:9–11. It facilitates the maintenance and sharing of law enforcement records. *Id.* at 47:5–15.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

26. TECS includes information about prior encounters between CBP officers and travelers at the U.S. border. Exh. 13 (CBP 30(b)(6) depo.) at 119:7–17.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

27. TECS includes “lookouts” created by CBP or other government agencies. Exh. 13 (CBP 30(b)(6) depo.) at 98:20–99:7; Exh. 14 (ICE 30(b)(6) depo.) at

211:14–22.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

28. A “lookout” is an alert about a traveler or vehicle that is entered into a database by CBP, ICE, or another law enforcement agency. Exh. 13 (CBP 30(b)(6) depo.) at 97:5–11; Exh. 14 (ICE 30(b)(6) depo.) at 205:2–23; Exh. 22 (CBP 2018 PIA) at Bates 177.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

29. At primary inspection, CBP officers query TECS to identify “lookouts” and recent border crossings. Exh. 13 (CBP 30(b)(6) depo.) at 85:14–86:24, 93:12–19.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

30. If a traveler has a “lookout,” the primary inspection CBP officer will refer the traveler to secondary inspection. Exh. 13 (CBP 30(b)(6) depo.) at 101:25–102:12; Exh. 14 (ICE 30(b)(6) depo.) at 206:19–207:19. A CBP officer may also refer the traveler to ICE. Exh. 14 (ICE 30(b)(6) depo.) at 205:2–23, 207:22–208:3, 209:6–210:2.

Defendants’ Response: Dispute characterization that all travelers with a “lookout” *will* be referred to secondary inspection. Admit that a “lookout” *may* result in a referral to secondary inspection.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. The CBP deposition testimony

states that a lookout “would” result in an individual being referred to secondary inspection. Exh. 13, ECF No. 91-12 (CBP 30(b)(6) depo.) at 101:25– 102:3, 102:8–12. The ICE deposition testimony states that a lookout “might” result in an individual being referred to secondary inspection. Exh. 14, ECF No. 91-13 (ICE 30(b)(6) depo.) at 206:19–207:19.

31. “Lookouts” can be a reason why some travelers are subjected to border searches of their electronic devices. Exh. 13 (CBP 30(b)(6) depo.) at 103:15–104:2, 208:5–10.

Defendants’ Response: Dispute plaintiff’s characterization that “travelers are subjected to border searches” but admit that “lookouts” can be a reason why CBP conducts a border search of an electronic device.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute.

32. “Lookouts” last as long as CBP deems them pertinent. Exh. 13 (CBP 30(b)(6) depo.) at 101:19–23.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

33. CBP officers use TECS to document border searches of electronic devices. Exh. 13 (CBP 30(b)(6) depo.) at 90:15–21, 119:18–21. This includes the officers’ reasons for search, *id.* at 125:19 –126:18, 151:5–11, and information the officers discover that they deem of law enforcement benefit, *id.* at 169:19–21. *See also* Exh. 22 (CBP 2018 PIA) at Bates 186.

Defendants’ Response: No dispute.

Plaintiffs' Reply: No dispute.

34. During secondary inspections, CBP officers consider information in TECS, including information about prior border screenings. Exh. 13 (CBP 30(b)(6) depo.) at 117:7– 119:21.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

35. When ICE agents are deciding whether to conduct a border search of an electronic device, they have access to information in TECS. Exh. 14 (ICE 30(b)(6) depo.) at 90:24–92:5.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

2. CBP's Automated Targeting System

36. CBP's Automated Targeting System ("ATS") uses "rules" to conduct risk assessments that "flag[]" certain travelers for "additional inspection." Exh. 13 (CBP 30(b)(6) depo.) at 107:7–25. *See also id.* at 104:11–14, 106:8–16; Exh. 23 (CBP 2017 ATS PIA) at Bates 997, 999, 1003.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

37. When assessing risk, ATS uses information from TECS. Exh. 13 (CBP 30(b)(6) depo.) at 107:22–25. *See also* Exh. 23 (CBP 2017 ATS PIA) at Bates 1000.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

38. ATS provides CBP officers with access to

dozens of other government databases. Exh. 23 (CBP 2017 ATS PIA) at Bates 997–99.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

39. If ATS flags a traveler, then a CBP officer conducting a primary inspection must refer the traveler to secondary inspection. Exh. 13 (CBP 30(b)(6) depo.) at 109:4–13.

Defendants’ Response: Dispute characterization and state that a CBP officer’s reason for referring a traveler to secondary inspection may be based upon a review of the results of an ATS risk assessment.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. The CBP deposition testimony states: “Q. So if ATS indicates that a traveler should be referred to secondary inspection, does the officer at primary have any discretion in deciding whether to refer that person? A. No. It’s a lookout that’s – that informs the primary officer.” Exh. 13, ECF No. 91-12 (CBP 30(b)(6) depo.) 109:8–13.

40. If an advanced search of an electronic device yields information that a CBP officer deems of law enforcement benefit, then the officer will copy it into ATS. Exh. 13 (CBP 30(b)(6) depo.) at 104:18–105:2; Exh. 22 (CBP 2018 PIA) at Bates 184, 186; Exh. 23 (CBP 2017 ATS PIA) at Bates 1034; Exh. 27 (DHS OIG 2018 Report) at Bates 975.

Defendants’ Response: Dispute characterization and state that articulated in the ATS PIA, Bates 0996, a CBP Officer is

authorized to include information from the border search of an electronic device in ATS if the subject of the search is of significant law enforcement, counterterrorism, or national security concerns.

Plaintiffs' Reply: No dispute.

41. ATS stores copies of data from travelers' devices, not officers' narrative descriptions of that data. Exh. 13 (CBP 30(b)(6) depo.) at 190:10–19.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

42. ATS stores copies of data from travelers' devices for 15 years or “the life of the law enforcement matter,” whichever is longer. Exh. 23 (CBP 2017 ATS PIA) at Bates 1037.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

43. ATS may use the information copied from a traveler's device to flag the traveler for heightened screening in the future. Exh. 13 (CBP 30(b)(6) depo.) at 114:10– 18, 115:12–25; Exh. 22 (CBP 2018 PIA) at Bates 184; Exh. 23 (CBP 2017 ATS PIA) at Bates 1034.

Defendants' Response: No dispute that Officers may flag a traveler for additional scrutiny on the basis of information maintained in ATS.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. The CBP deposition testimony states: “Q. Does information obtained from border searches of electronic devices affect how

ATS flags individuals for additional scrutiny at the border? A. I think it could.” Exh. 13, ECF No. 91-12 (CBP 30(b)(6) depo.) at 114:10–14.

44. When ICE agents decide whether to conduct a border search of an electronic device, they have access to ATS. Exh. 14 (ICE 30(b)(6) depo.) at 99:4–10.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

3. ICE’s Investigative Case Management

45. ICE operates a database called Investigative Case Management (“ICM”). Exh. 14 (ICE 30(b)(6) depo.) at 163:20–164:4.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

46. ICM contains (a) “reports of investigation,” and (b) “subject records,” which identify people and things that are connected to investigations. Exh. 14 (ICE 30(b)(6) depo.) at 164:13–165:8.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

47. ICM contains nearly all of ICE’s case information. Exh. 14 (ICE 30(b)(6) depo.) at 160:3–13.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

48. When ICE agents decide whether to conduct border searches of electronic devices, they have access to ICM information. Exh. 14 (ICE 30(b)(6) depo.) at 164:5–12.

Defendants’ Response: No dispute.

Plaintiffs' Reply: No dispute.

49. ICM information that can be relevant to whether to conduct a border search of an electronic device includes prior encounters between ICE and travelers at the border, including whether travelers were subjected to device searches. Exh. 14 (ICE 30(b)(6) depo.) at 166:13– 168:14.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

50. If an ICE agent conducts a border search of an electronic device, they may use an ICM report of investigation to store information about what they found. Exh. 14 (ICE 30(b)(6) depo.) at 169:10–22. ICM contains an agent's descriptions of data in a traveler's device, but not the data itself. *Id.* at 172:5–14. This may include, for example, a “verbatim transcript of a conversation,” or a “summary” of a conversation or a photograph. *Id.* at 172:15–174:11.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

51. ICM information about the contents of travelers' devices can be relevant to whether to conduct a future border search of an electronic device. Exh. 14 (ICE 30(b)(6) depo.) at 174:12–24.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

II. The Frequency of Border Searches and Confiscations of Electronic Devices

A. Defendants' Statistical Data

52. CBP conducted the following total number of border searches of electronic devices during each fiscal year (“FY”) from 2012 through 2018:

- FY 2012: 5,085
- FY 2013: 5,709
- FY 2014: 6,029
- FY 2015: 8,503
- FY 2016: 19,051
- FY 2017: 30,524
- FY 2018: 33,295

Exh. 46 (Stipulations) at ¶ 13.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

53. CBP conducted the following number of basic searches of electronic devices at the border during each fiscal year from 2012 through 2018:

- FY 2012: 3,182
- FY 2013: 3,561
- FY 2014: 4,314
- FY 2015: 6,618
- FY 2016: 16,914
- FY 2017: 27,701
- FY 2018 (through September 15, 2018): 28,429¹

Exh. 26 (Defs. Interrog. Responses) at #6.

Defendants’ Response: No dispute.

Plaintiffs' Reply: No dispute.

54. CBP conducted the following number of advanced searches of electronic devices at the border during each fiscal year from 2012 through 2018:

- FY 2012: 2,285
- FY 2013: 2,444
- FY 2014: 1,921
- FY 2015: 2,090
- FY 2016: 2,394
- FY 2017: 2,685
- FY 2018 (through September 15, 2018): 3,485

Exh. 26 (Def. Interrog. Responses) at #6.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

55. CBP conducted the following number of confiscations of travelers' electronic devices after they left ports of entry during each fiscal year from 2012 through 2018.

- FY 2012: 8
- FY 2013: 36
- FY 2014: 32
- FY 2015: 21
- FY 2016: 131
- FY 2017: 200
- FY 2018 (through September 15, 2018): 172

Exh. 26 (Def. Interrog. Responses) at #6.

Defendants’ Response: Dispute the characterization of the fact because the wording differs from the wording used in Defendants’ Response to Interrogatory 6. Defendants do not dispute that that CPB estimated that it “detained the [above] number of electronic devices after a traveler departed the port of entry or other location of inspection in each of the identified fiscal years.”

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. For clarification, Defendants say “detained” devices and Plaintiffs say “confiscated” devices after a traveler has left the border.

B. Defendants’ Statistics Do Not Reflect All Border Searches and Confiscations of Electronic Devices

56. ICE does not maintain records of the number of basic searches of electronic devices that it conducts. Exh. 46 (Stipulations) at ¶ 14.

Defendants’ Response: Dispute that this is a material fact as the number of basic searches conducted by ICE or whether ICE records those numbers is not material to the constitutionality of border searches of electronic devices.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. The number of basic searches that ICE conducts is material to Plaintiffs’ standing. *See* Pls.’ Mem. in Support of their Mot. for Sum. Judgment, ECF No. 90-1 (“Pl. Br.”) at Part IV.B. To the extent that

Defendants rely on a baseline probability of a device search based on the number of device searches they have recorded, undercounting or a failure to record basic searches affects the likelihood of a risk of future device search. Defendants do not dispute the accuracy of the fact itself.

57. ICE agents may conduct basic searches of electronic devices. Exh. 29 (DHS 2009 PIA) at Bates 224.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

58. ICE does not maintain records of the number of times it detains electronic devices after travelers leave ports of entry. Exh. 14 (ICE 30(b)(6) depo.) at 330:2–10.

Defendants' Response: Dispute plaintiffs' characterization of the cited testimony. ICE records every instance that an electronic device is detained for a border search; it does not record those occurrences in a manner that permits for aggregable statistics. *Id.* at 331:6 – 332:6. Further dispute this is a material fact as the number of basic searches conducted by ICE or whether ICE records those numbers is not material to the constitutionality of border searches of electronic devices.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. Defendants' assertion that ICE does not record device detentions "in a manner that permits for aggregable statistics" is effectively the same as not maintaining

records at all. This is a material fact that goes to Plaintiffs' standing because it relates to the likelihood of risk of future device detention or confiscation after a traveler has left the border. *See* Pl. Br. at Part IV.B.

59. CBP determines the number of border searches of electronic devices in a given period by calculating the number of closed or completed Electronic Media Reports ("EMRs"). Exh. 26 (Defs. Interrog. Responses) at #11. EMRs are sometimes called "IOEMs." Exh. 13 (CBP 30(b)(6) depo.) at 201:7–9.

Defendants' Response: No dispute, except to dispute this is a material fact.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact that goes to Plaintiffs' standing because it relates to the likelihood of risk of future device search. *See* Pl. Br. at Part IV.B.

60. CBP officers sometimes do not complete EMRs after conducting border searches of electronic devices. Exh. 27 (DHS OIG 2018 Report) at Bates 973, 978; Exh. 13 (CBP 30(b)(6) depo.) at 248:18–249:9.

Defendants' Response: Do not dispute that the 2018 DHS OIG report found, in the period of examination, that CBP officers sometimes did not complete EMRs. Further dispute that this is a material fact.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact that goes to Plaintiffs' standing because it relates to the likelihood of risk of future device search.

See Pl. Br. at Part IV.B.

61. For example, on August 28, 2017, CBP officers searched the smartphone they seized from Plaintiff Nadia Alasaad's bag. Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 73–74, Defendants have no records, including EMRs, documenting that search. Exh. 26 (Defs. Doc. Responses) at #17.

Defendants' Response: Dispute the inference being drawn by the fact that CBP does not have any records documenting that alleged search and further dispute that this is a material fact.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. Plaintiffs do not know what inference Defendants are referring to as being drawn; Plaintiffs cited to Defendants' discovery response. This fact presents one example of undercounting as to one Plaintiff. This is a material fact that goes to Plaintiffs' standing to the extent that standing considers the number of device searches as an indication of likelihood of risk of future device search. *See* Pl. Br. at Part IV.B.

62. When CBP officers do not fill out EMRs for border searches of electronic devices, those searches are not included in CBP's calculation of the total number of searches for that period. Exh. 26 (Defs. Interrog. Responses) at #11; Exh. 13 (CBP 30(b)(6) depo.) at 251:3– 15.

Defendants' Response: Dispute that this is a material fact.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact that

goes to Plaintiffs' standing because it relates to the likelihood of risk of future device search. See Pl. Br. at Part IV.B.

III. Privacy Implications of Device Searches

A. The Sensitivity of Content in Travelers' Devices

63. Electronic devices carried by travelers, such as smartphones or laptops, can contain a very large volume of information. Exh. 13 (CBP 30(b)(6) depo.) at 161:25–162:3; Exh. 14 (ICE 30(b)(6) depo.) at 212:21–213:3.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

64. Travelers carry electronic devices that contain many different kinds of information, such as photos, contacts, emails, and text messages, and the devices may reveal such things as prescription information, information regarding employment, travel history, and browsing history. Exh. 13 (CBP 30(b)(6) depo.) at 161:21–24, 164:3–13, 167:12–17, 191:10–14; Exh. 14 (ICE 30(b)(6) depo.) at 213:5–8.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

65. A CBP training document describes border searches of electronic devices as “very sensitive.” Exh. 31 (Pilot Program for CBP 2018 Directive) at Bates 143.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

66. ICE recognizes that electronic devices have the capacity to “store sensitive information.” Exh. 29 (DHS 2009 PIA) at Bates 231.

Defendants' Response: No dispute

Plaintiffs' Reply: No dispute.

B. The Invasiveness of Manual and Forensic Device Searches

67. Basic searches can access content from allocated space physically resident on an electronic device that is accessible using the native operating system of the device, including but not limited to its native graphical user interface and/or touchscreen. Exh. 46 (Stipulations) at ¶ 2.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

68. Basic searches can extend to any allocated file or information that is resident on the device and accessible using the device's native operating system. Exh. 46 (Stipulations) at ¶ 4.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

69. Separate from the primary content stored on them, some electronic devices may also store data related to that content, such as the date and time associated with the content, usage history, sender and receiver information, or location data. That content may be revealed during a basic search, depending on the type of device, the operating system, the relevant settings, and the applications used to create and/or

maintain the data. Exh. 46 (Stipulations) at ¶ 5.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

70. When conducting a basic search, officials are able to use the native search functions in the native operating system of the device, such as a key word search tool, if there is one. Exh. 46 (Stipulations) at ¶ 3.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

71. A device's internal search tools can be used to search for particular words and images. Exh. 14 (ICE 30(b)(6) depo.) at 214:24–216:10, 216:25–217:4, 218:9–20, 219:16– 221:11.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

72. Depending on the equipment, procedures, and techniques used, advanced searches of electronic devices are generally capable of revealing everything a basic search may reveal. Exh. 46 (Stipulations) at ¶ 6.

Defendants' Response: No dispute, except dispute that it is material.

Plaintiffs' Reply: Defendants raise no genuine dispute. This is a material fact because it relates to travelers' privacy interests under the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.1.

73. An advanced search of an electronic device, depending on the equipment, procedures, and

techniques used, may be capable of revealing deleted or other data in unallocated storage space and password-protected or encrypted data. Exh. 46 (Stipulations) at ¶ 8. *See also* Exh. 13 (CBP 30(b)(6) depo.) at 298:3–17.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

74. An advanced search of an electronic device may be able to copy all information physically resident on the device or may be limited to only certain files, depending on the search equipment, procedures, and techniques used. Exh. 46 (Stipulations) at ¶ 12. *See also* Exh. 13 (CBP 30(b)(6) depo.) at 205:13–23.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

75. If information from the internet is cached on a device, such as web-based email, and the device is disconnected from the internet, border officers can still search the cached information. Exh. 14 (ICE 30(b)(6) depo.) at 222:9–223:15; Exh. 13 (CBP 30(b)(6) depo.) at 186:2–24.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

76. Some CBP officers may have accessed cloud-based content during searches of electronic devices, even after issuance of an April 2017 memorandum requiring that officers disable network connectivity prior to search, because more than one-third of EMRs lacked a statement confirming that the device’s data connection had been disabled. Exh. 27 (DHS OIG 2018 Report) at Bates 979–980.

Defendants' Response: Do not dispute that the 2018 DHS OIG report concluded that based on EMRs reviewed in the stated time period that some CBP officers did not document that they had disabled network connectivity prior to a search during the time period examined, which was after issuance of an April 2017 memorandum requiring that officers disable network connectivity prior to search. Dispute that this is a material fact.

Plaintiffs' Reply: Defendants raise no genuine dispute. Plaintiffs refer the Court to the cited materials. This is a material fact because it relates to travelers' privacy interests under the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.1.

C. Privacy Risks From Retention of Information

77. To the extent consistent with applicable system of records notices, ICE and CBP can retain information from a device in any of their record keeping systems when an electronic device search reveals information officers deem relevant to immigration, customs, or other laws enforced by the Department of Homeland Security. Exh. 46 (Stipulations) at ¶ 10.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

78. ICE generally stores information from travelers' devices in ICE's Investigative Case Management System, and the rules for that database do not limit storage of this information, beyond the

requirement of relevance to immigration, customs, or other law enforcement matters. Exh. 14 (ICE 30(b)(6) depo.) at 323:16– 324:4, 326:18–327:4.

Defendants’ Response: Dispute to the extent this statement suggests that exact or complete electronic copies of an electronic device’s data are stored in ICM. Do not dispute that an ICE Special Agent can manually record a narrative description of information observed during a search of an electronic device in ICM. *Id.* at 324:16-325:2; 326:15-327:4.

Plaintiffs’ Reply: No dispute.

79. After a border search of an electronic device, the information contained on the device may be shared with other federal agencies for law enforcement and intelligence purposes. Exh. 13 (CBP 30(b)(6) depo.) at 44:18–45:12, 198:20–199:5; Exh. 30 (ICE 2007 Memorandum) at Bates 1265.

Defendants’ Response: Dispute plaintiffs’ characterization of this fact and refer Court to cited exhibits which make clear that the information sharing is permitted only if the information is related to immigration, customs, and other enforcement matters and if the sharing is consistent with applicable system of record notices. *See* Ex. 19 at 5.5.1.3 and 5.5.1.4; *see also* DHS/CBP/PIA-008(a) Border Searches of Electronic Devices at Bates 0174 (Ex. G); DHS/CBP/PIA-006(e) ATS at Bates 0996 (Ex. K).

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. In Defendants’ citations to Exh. 19, ECF No. 91-18 (CBP 2018 Directive) at

§§ 5.5.1.3 and 5.5.1.4, Bates 122, neither section has a clause stating that information sharing must be “related to immigration, customs, and other enforcement matters” or that sharing must be “consistent with applicable system of record notices.” However, Plaintiffs do not dispute that these limitations appear in § 5.5.1.2 as they pertain to retention. *See id.* at Bates 121–22. To clarify, Defendants do not dispute that subject to these limitations, information contained on an electronic device may be shared with other federal agencies for law enforcement and intelligence purposes.

80. After a border search of an electronic device, information retained in the TECS database may be shared with other agencies outside of DHS, including local, state, and foreign governments. Exh. 13 (CBP 30(b)(6) depo.) at 83:18–84:17; 198:11–19.

Defendants’ Response: Dispute plaintiffs’ characterization of this fact and refer Court to cited exhibits which make clear that the information sharing is permitted only if the information is related to immigration, customs, and other enforcement matters and if the sharing is consistent with applicable system of record notices.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. Defendants have provided no support for their assertion. However, Plaintiffs do not dispute that these limitations appear in § 5.5.1.2 as they pertain to retention. *See* Exh. 19, ECF No. 91-18 (CBP 2018 Directive) at § 5.5.1.2, at Bates 121–22. To clarify, Defendants do not dispute that subject to these limitations,

information contained on an electronic device may be shared with other agencies outside of DHS, including local, state, and foreign governments. *See also* Exh. 13, ECF No. 91-12 (CBP 30(b)(6) depo.) at 198:11–19 (“Q. So this policy permits the sharing of information from electronic devices searched at the border with state, local, foreign governments; is that correct? A. That’s what it says. Q. And, in fact, CBP does share information from electronic devices with those other Government entities at times; is that right? A. We do.”).

IV. Government Interests

A. Defendants’ Asserted Purposes

81. CBP and ICE assert authority to conduct warrantless or suspicionless border searches of electronic devices to enforce hundreds of federal laws. Exh. 19 (CBP 2018 Directive) at Bates 115; Exh. 22 (CBP 2018 PIA) at Bates 189; Exh. 14 (ICE 30(b)(6) depo.) at 28:4–6.

Defendants’ Response: This is a conclusion of law and not a material fact. If deemed a material fact, no dispute.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. That Defendants assert authority to conduct warrantless or suspicionless border searches of electronic devices to enforce hundreds of federal laws is not a legal conclusion but rather a fact. This is a material fact because the government’s asserted authority to conduct warrantless, suspicionless border searches of electronic devices is at the heart of the dispute in this

lawsuit.

82. CBP's asserted purposes in conducting warrantless or suspicionless border searches of electronic devices include general law enforcement, *i.e.*, finding potential evidence of illegal activity beyond violations of immigration and customs laws. Exh. 26 (Defs. Interrog. Responses) at #1 (“[B]order searches of electronic devices are conducted in furtherance of . . . law enforcement[] and homeland security responsibilities and to ensure compliance with . . . other laws that Defendants are authorized to enforce and administer. . . . They are a crucial tool for detecting evidence relating to terrorism and other national security matters . . . They can also reveal information about financial and commercial crimes. . . .”). *See also* Exh. 19 (CBP 2018 Directive) at § 1, Bates 113; Exh. 13 (CBP 30(b)(6) depo.) at 20:19–21:9, 32:23–33:6; Exh. 33 (CBP “Tear Sheet”) at Bates 163 (“domestic law enforcement”); Exh. 23 (CBP 2017 ATS PIA) at Bates 1034 (“other enforcement matters”) & 1035 (“other laws enforced by CBP”); Exh. 27 (DHS OIG 2018 Report) at Bates 975 (“any violation of laws”), 981 (“law enforcement-related information”), 982 (use of “new technologies to commit crimes”); Exh. 34 (CBP Written Statement for the Record for Senate Homeland Security Committee, July 11, 2018) at Bates 277 (use of “new technologies to commit crimes”); Exh. 35 (CBP Instructor Guide—P180C) at Bates 1279.

Defendants’ Response: Dispute plaintiffs’ characterization that CBP’s asserted purpose for conducting border searches include general law enforcement. The cited exhibits demonstrate that CBP officers’ searches are

related to the agency's broad law enforcement and national security responsibilities. *See also* 6 U.S.C. § 211.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. The cited evidence demonstrates the number and various types of situations in which CBP asserts that warrantless, suspicionless searches of electronic devices advance law enforcement purposes.

83. ICE's asserted purposes for warrantless or suspicionless border searches of electronic devices include general law enforcement, *i.e.*, finding potential evidence of illegal activity beyond violations of immigration and customs laws. Exh. 26 (Defs. Interrog. Responses) at #1; Exh. 21 (ICE 2009 Directive) at § 4, Bates 261 ("other Federal laws at the border"); Exh. 30 (ICE 2007 Memorandum) at Bates 1264 ("anything that may be evidence of a crime"); Exh. 14 (ICE 30(b)(6) depo.) at 35:15–17, 36:23–37:5, 40:10–20.

Defendants' Response: Dispute plaintiffs' characterization that ICE's asserted purpose for conducting border searches include general law enforcement and for finding illegal activity beyond violations of immigration and customs laws. The cited exhibits demonstrate that ICE agents' searches are related to the agency's broad law enforcement and national security responsibilities. *See also* 6 U.S.C. §§ 202, 251-52.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. The cited evidence

demonstrates the number and various types of situations in which ICE asserts that warrantless, suspicionless searches of electronic devices advance law enforcement purposes.

84. ICE asserts that agents may conduct a warrantless or suspicionless border search of the electronic device of a traveler:

- a. Who is suspected of violating tax laws, to find emails reflecting the tax law violations. Exh. 14 (ICE 30(b)(6) depo.) at 29:4–8, 31:5–12.
- b. Who is suspected of hiding assets in bankruptcy, to find emails reflecting the hiding of assets. *Id.* at 33:4–22.
- c. Who is an executive of a company suspected of criminally dumping toxins into a river, to find emails reflecting the illegal dumping. *Id.* at 31:14–23, 32:2–8.
- d. Who is suspected of violating consumer protection laws, to find evidence reflecting the consumer protection law violations. *Id.* at 32:10–33:2.
- e. Who is suspected of money laundering, to find emails or other evidence reflecting money laundering, including the creation of corporations and accounts and the structuring of deposits. *Id.* at 41:3–42:13.

Defendants’ Response: Dispute the characterizations of the deposition testimony which make clear that border searches of an individual under any of the above

circumstances would only be conducted if ICE was also investigating that individual for violation of a cross-border crime within the jurisdiction of ICE. *Id.* at 52:4–14.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. Plaintiffs refer the Court to the cited materials.

85. CBP and ICE’s asserted purposes in conducting warrantless or suspicionless border searches of electronic devices include finding potential evidence of customs violations, including evidence of importing or exporting contraband, in contrast to finding contraband itself. Exh. 26 (Defs. Interrog. Responses) at #1 (“detecting evidence relating to . . . human and bulk cash smuggling, contraband, and child pornography”); Exh. 13 (CBP 30(b)(6) depo.) at 62:19– 21; Exh. 35 (CBP Instructor Guide—P180C) at Bates 1279 (“evidence related to . . . [h]uman/cash smuggling” and “[n]arcotics and contraband”); Exh. 36 (ICE/HSI Priority Requests) at Bates 93 (“. . . if an individual is encountered smuggling methamphetamine . . . a border search would be conducted on his devices for co-conspirators”).

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

86. CBP and ICE’s asserted purposes in conducting warrantless or suspicionless border searches of electronic devices include intelligence gathering. Exh. 13 (CBP 30(b)(6) depo.) at 46:24–47:3, 47:16–48:7; Exh. 23 (CBP 2017 ATS PIA) at Bates 1003, 1034; Exh. 30 (ICE 2007 Memorandum) at Bates 1265 (“intelligence interest[s]”).

Defendants’ Response: Dispute that the cited references support plaintiffs’ characterization of Defendants’ purposes for conducting border searches. Defendants refer the Court to the referenced documents which, for the most part, discuss the agencies’ record keeping systems. In addition, Exh 30 does not state that intelligence gathering is a purpose of border searches. *Id.* at 1264 (stating that the two general objectives of a border search is “to inspect for merchandise imported contrary to law” and “to obtain information or evidence relating to an individual’s admissibility.”); *See also* Defs.’ Response to Pls.’ First Set of Interrog, Interrog. No.1 (Ex. I).

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. Exh. 26, ECF No. 91-25 (Def. Interrog. Responses) at #1 states that warrantless, suspicionless border searches of electronic devices “are a crucial tool for detecting evidence related to ... national security matters.” Moreover, the CBP deposition testimony and ATS PIA together show that device data is uploaded to ATS, and ATS is used for intelligence purposes. Exh. 13 (CBP 30(b)(6) depo.) at 46:24–47:3, 47:16–48:7; Exh. 23 (CBP 2017 ATS PIA) at Bates 1003, 1034. Additionally, Exh. 33, ECF No. 91-32 (CBP “Tear Sheet”) at Bates 163 lists “ROUTINE USES” including “border security and intelligence activities.”

87. CBP’s decisions to conduct warrantless or suspicionless border searches of electronic devices are informed by information or requests from other

government agencies. Exh. 26 (Defs. Interrog. Responses) at #17 (“CBP decisions to perform border searches of electronic devices benefit from information provided by other law enforcement agencies”); Exh. 13 (CBP 30(b)(6) depo.) at 75:8–76:5, 76:11–25, 77:13–14, 83:18–84:12; Exh. 37 (CBP Briefing for Senate Committee) at Bates 288 (“CBP coordinates with FBI”).

Defendants’ Response: No dispute, except to dispute that this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact because it is relevant to evaluating the government’s interest under the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.

88. ICE’s decisions to conduct warrantless or suspicionless border searches of electronic devices are informed by information or requests from other government agencies. Exh. 26 (Defs. Interrog. Responses) at #17. *See also* Exh. 14 (ICE 30(b)(6) depo.) at 189.9–190:21, 191:18–192:3. These agencies include the Bureau of Alcohol, Tobacco, Firearms and Explosives, Internal Revenue Service, Secret Service, Federal Bureau of Investigation, State Department, state and local police departments and county sheriffs, and foreign law enforcement agencies. Exh. 14 (ICE 30(b)(6) depo.) at 194:13–201:25.

Defendants’ Response: Dispute plaintiffs’ characterization of the cited evidence but do not dispute that the cited evidence shows that ICE makes independent determinations on the necessity for every border search they undertake and that information provided by

other law enforcement agencies *may* inform the agency's decision to conduct a border search of an electronic device. *See also* Exh. 26. at No. 17. Further dispute that this is material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact because it is relevant to evaluating the government's interest under the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.

89. CBP asserts it may conduct warrantless or suspicionless border searches of electronic devices when the subject is someone other than the traveler. Exh. 13 (CBP 30(b)(6) depo.) at 57:3–17 (another person's crime), 58:6–59:9 (same), 59:11–60:10 (another person's admissibility).

Defendants' Response: No dispute except to clarify that CBP has authority to search any traveler at the border and CBP policies permit a basic search of an electronic device with or without suspicion.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. Defendants' statement that "CBP has authority to search any traveler at the border" is a legal assertion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: no dispute. Plaintiffs clarify that Defendants' border search authority is subject to statutory and constitutional limits.

90. ICE asserts that warrantless or suspicionless border searches of electronic devices may be conducted when the subject of interest is

someone other than the traveler. This includes:

- a. When the traveler is a U.S. citizen and ICE is seeking information about a suspected undocumented immigrant. Exh. 14 (ICE 30(b)(6) depo.) at 64:18–65:19.
- b. When the traveler is a reporter who is known to have had contact with a suspected terrorist, where there is no suspicion that the reporter engaged in wrongdoing. Exh. 14 (ICE 30(b)(6) depo.) at 56:25–58:14. *See also id.* at 74:14–75:6.
- c. When the traveler is a journalist or a scholar with foreign sources who are of interest to the U.S. government. Exh. 14 (ICE 30(b)(6) depo.) at 75:14–25.
- d. When the traveler is business partners with someone who is under investigation for tax fraud. Exh. 14 (ICE 30(b)(6) depo.) at 50:15–51:4.
- e. When the traveler is a family member of a person under investigation, in conjunction with other factors. Exh. 14 (ICE 30(b)(6) depo.) at 130:16– 131:3.

Defendants’ Response: Dispute plaintiffs’ characterization of the cited evidence and clarify that ICE has the authority to search an electronic device of any traveler at the border in furtherance of its mission.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. Defendants’ statement that “ICE has the authority to search an electronic device of any traveler at the border in

furtherance of its mission” is a legal assertion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: no dispute that ICE claims such authority, but Plaintiffs clarify that Defendants’ border search authority is subject to statutory and constitutional limits.

91. CBP and ICE conduct warrantless or suspicionless border searches of electronic devices to advance pre-existing investigations. Exh. 35 (CBP Instructor Guide— P180C) at Bates 1281 (“ongoing INVESTIGATIONS”); Exh. 26 (Defs. Interrog. Responses) at #16 (“the potential for that search to further a particular investigation”); Exh. 14 (ICE 30(b)(6) depo.) at 193:2–15; Exh. 29 (DHS 2009 PIA) at Bates 222.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

B. Digital Contraband at the Border

92. Child pornography is primarily transferred into the United States via the internet. Exh. 14 (ICE 30(b)(6) depo.) at 297:9–12.

Defendants’ Response: Dispute that this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact because it is relevant to evaluating the government’s interest under the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.

93. ICE considers few things to be digital

contraband: child pornography, malware, information that cannot lawfully be exported, and unreported digital currency. Exh. 14 (ICE 30(b)(6) depo.) at 37:25–38:24, 39:3–19.

Defendants’ Response: Dispute that this is an exhaustive list of digital contraband and further dispute that this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. The ICE deposition testimony states: “Q. Okay, So other than the three examples you’ve given now — the child pornography, ... the export control violation and the malware exploit — are you aware of any other examples of digital information on a traveler’s of digital information on a traveler’s device that, of itself, would be illegal contraband? A. That’s all I can think of right now.” Exh. 14 (ICE 30(b)(6) depo.) at 40:2–9. This is a material fact because it is relevant to evaluating the government’s interest under the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.

94. CBP cannot identify any type of digital contraband beyond child pornography. Exh. 13 (CBP 30(b)(6) depo.) at 62:8–66:15.

Defendants’ Response: Dispute plaintiffs’ characterization of the deposition testimony. Howe Declaration (Ex. A) ¶ __.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. Plaintiffs refer the Court to the pages listed in the CBP deposition testimony, in which after repeated questioning, the deponent was only able to identify child

pornography as the sole example of digital contraband. *See* Exh. 13, ECF No. 91-12 (CBP 30(b)(6) depo.) at 62:8–66:15.

95. Digital data can be posted, shared, or transmitted via the internet and stored on an electronic device. Exh. 46 (Stipulations) at ¶ 9.

Defendants’ Response: No dispute, except dispute that it is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact because it is relevant to evaluating the government’s interest under the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.

96. Defendants are aware that digital contraband may in certain circumstances be accessible from the United States via the internet. Exh. 26 (Defs. Interrog. Responses) at #5.

Defendants’ Response: Dispute that this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact because it is relevant to evaluating the government’s interest under the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.

97. ICE acknowledges that child pornography can enter or be viewed in the United States via the internet in many ways:

- a. By viewing content on servers located outside the United States.
- b. Exh. 14 (ICE 30(b)(6) depo.) at 286:5–13.
- c. As email attachments. *Id.* at 286:15–19.

- d. As text messages. *Id.* at 286:20–25.
- e. Via live streaming. *Id.* at 288:20–289:7.
- f. Via a listserv or chat group. *Id.* at 289:20–24.
- g. Via the Dark Web. *Id.* at 290:7–9.

Defendants’ Response: Dispute that this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact because it is relevant to evaluating the government’s interest under the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.

98. When Defendants confiscate digital contraband at the border, they either (a) cannot determine whether that digital contraband is already present in the United States, or (b) can determine, through a method known as “hashing,” that the digital contraband is already present in the United States. Exh. 14 (ICE 30(b)(6) depo.) at 299:5– 24.

Defendants’ Response: Dispute that defendants “confiscate” digital contraband and that this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact because it is relevant to evaluating the government’s interest under the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.

C. **Lack of Evidence That Defendants’ Policies and Practices Are Effective**

99. CBP and ICE do not know how many warrantless or suspicionless border searches of

electronic devices uncover digital contraband. Exh. 26 (Def. Interrog. Responses) at #13; Exh. 13 (CBP 30(b)(6) depo.) at 68:10–14; Exh. 14 (ICE 30(b)(6) depo.) at 44:25–45:7.

Defendants’ Response: Dispute that this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact because it is relevant to evaluating the government’s interest under the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.

100. CBP and ICE do not know how many warrantless or suspicionless border searches of electronic devices uncover potential evidence of criminal activity. Exh. 13 (CBP 30(b)(6) depo.) at 68:15–20; Exh. 14 (ICE 30(b)(6) depo.) at 338:18–24.

Defendants’ Response: Dispute that this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact because it is relevant to evaluating the government’s interest under the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.

101. CBP does not know how many warrantless or suspicionless border searches of electronic devices result in prosecution or conviction. Exh. 27 (DHS OIG 2018 Report) at Bates 982.

Defendants’ Response: Dispute that this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact because

it is relevant to evaluating the government's interest under the Fourth Amendment balancing test. See Pl. Br. at Part I.A.2.

102. ICE does not know how many warrantless or suspicionless border device searches result in criminal arrests or indictments, or referrals to other law enforcement agencies. Exh. 36 (ICE/HSI Priority Requests) at Bates 93.

Defendants' Response: Dispute plaintiffs' characterization of the cited evidence because the referenced exhibit provides statistics for arrests, indictments, seizures, search warrants, and administrative arrests resulting from investigations that included a border search of an electronic device. Bates 0094. Also dispute that this is a material fact.

Plaintiffs' Reply: Dispute Defendants' characterization of the evidence. The referenced exhibit states: “[Q.] By year, please identify the number of criminal arrests, indictments by nearly [sic], search warrants, and/or seizures occurred based upon, in part, the screening of an individual's electronic device. [A.] There is no feasible way to produce meaningful statistics for this request. While a number could be produced that identified cases where a border search of an electronic device was conducted, *that may not be indicative that the search supported any particular arrest, indictment, search warrant, or seizure.* HSI Investigations involve a myriad of factors that would justify an arrest, indictment, or search warrant of which a border search would be only one factor of many.” Exh. 36, ECF No. 91-35

(ICE/HSI Priority Requests) at Bates 93 (emphasis added). There is a difference between (1) a border search of an electronic device search *resulting in* criminal arrests or indictments and (2) criminal arrests or indictments “resulting from *investigations that included* a border search of an electronic device” (emphasis added), because in the latter situation, the border search of an electronic device may not have contributed at all to the ultimate arrest or indictment. The statistics that Defendants cite to involve the latter situation. *See* Exh. 51 at Bates 94. This is a material fact because it is relevant to evaluating the government’s interest under the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.

D. CBP and ICE Obtain Warrants and Apply a Reasonable Suspicion Standard

1. CBP Obtains Warrants

103. CBP sometimes conducts searches of electronic devices pursuant to warrants. Exh. 38 (Border Patrol 2018 Digital Forensics Program PIA) at Bates 1130–31.

Defendants’ Response: Dispute plaintiffs’ characterization of cited document which applies only when agency employees in a separate operational office within CBP are not operating pursuant to border search authority. Further dispute that this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. It is irrelevant that this fact

pertains to when CBP is not operating pursuant to border search authority. This fact merely states that there are situations in which CBP is familiar with obtaining warrants for searches of electronic devices. This is a material fact because it is relevant to the application of the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.c.

104. CBP sometimes applies a probable cause standard for the seizure of an electronic device. Exh. 13 (CBP 30(b)(6) depo.) at 260:11–15.

Defendants’ Response: Dispute plaintiffs’ characterization of the fact and refer to the CBP Directive which specifies that 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 the device, or copy of the contents of the device, contains evidence of a violation of a law that CBP is authorized to enforce or administer. *See* Exh. 19 at 5.5.1.1. Further dispute that this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. The CBP 2018 Directive contemplates probable cause based “on other facts and circumstances.” Exh. 19, ECF No. 91-18 (CBP 2018 Directive) at § 5.5.1.1, Bates 121. This is a material fact because it is relevant to the application of the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.c.

105. CBP provides officers written guidance and

training on what constitutes probable cause. Exh. 13 (CBP 30(b)(6) depo.) at 260:16–261:16. CBP also provides training on how to obtain warrants. *Id.* at 279:25–280:4.

Defendants’ Response: Dispute plaintiffs’ characterization of the fact. Although officers are provided guidance and training on probable cause and warrants, it is only for specific situations and as it relates to certain distinct legal authorities (other than border search authority) under which CBP officers may operate. Further, dispute that this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. It is irrelevant that this fact pertains to when CBP is not operating pursuant to border search authority. This fact merely states that there are situations in which CBP demonstrates familiarity with the probable cause standard and how to obtain warrants. This is a material fact because it is relevant to the application of the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.c.

106. CBP sometimes obtains warrants for searches of international mail. Exh. 13 (CBP 30(b)(6) depo.) at 267:3–5. Specifically, if the officer has reasonable suspicion that a sealed parcel contains contraband, they may open it, but still need a warrant to read any correspondence. *Id.* at 268:12–25, 270:20–271:7; Exh. 39 (2001 International Mail Handbook) at Bates 1269. Without reasonable suspicion of contraband, CBP needs a warrant to open the mail. Exh. 13 (CBP 30(b)(6) depo.) at 268:12–25; 270:20–271:7; *see also* Exh. 39 (2001 International Mail

Handbook) at Bates 1269.

Defendants' Response: Dispute plaintiffs' characterization of the deposition testimony and cited exhibits. Admit that CBP sometimes works with other agencies to obtain warrants for searches of international mail and that in limited situations, officers need a warrant to read correspondence contained in sealed letter class mail that is transmitted within the international postal system and not letters carried by individuals or private carriers. Further dispute that this is a material fact.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. The 2001 International Mail Operations and Enforcement Handbook states: “[A] search warrant shall be obtained before any correspondence is read, seized, or referred to another agency . . . Customs would need to get a search warrant based on coherent facts before the correspondence could be read and used as evidence in the case.” Exh. 39, ECF No. 91-38 (2001 International Mail Handbook) at Bates 1269. This is a material fact because it is relevant to the application of the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.c.

107. Although CBP must obtain a warrant to read correspondence in international mail, CBP asserts it may read correspondence on an electronic device without any suspicion. Exh. 13 (CBP 30(b)(6) depo.) at 278:14–20.

Defendants' Response: Dispute plaintiffs' characterization of the testimony and refer to

the International Mail handbook (Exh. 39) for an accurate interpretation of the policy. The policy applies only when sealed international letter-class mail is in the custody of the postal service. It does not apply to border searches. Further dispute that this is a material fact.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. Plaintiffs do not assert that the 2001 International Mail Operations and Enforcement Handbook applies to ports of entry, but rather that international mail inspection occurs in a customs setting, where a warrant is required to read correspondence. This is a material fact because it is relevant to the application of the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.c.

108. CBP officers sometimes obtain warrants at the border to conduct:

- a. Involuntary x-ray searches. Exh. 13 (CBP 30(b)(6) depo.) at 262:13–17; Exh. 40 (CBP 2004 Personal Search Handbook) at § 6.h., Bates 1095.
- b. Involuntary body cavity searches. Exh. 13 (CBP 30(b)(6) depo.) at 263:13–15; Exh. 40 (CBP 2004 Personal Search Handbook) at § 8.I.d., Bates 1101.
- c. Prolonged detentions for medical examinations. Exh. 40 (CBP 2004 Personal Search Handbook) at § 2.p., Bates 1076.

Defendants' Response: Dispute characterization of the Handbook and refer court to the document for an accurate

statement of its contents. Further, dispute that this is a material fact.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact because it is relevant to the application of the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.c.

109. CBP's Air and Marine Operations is required to get a warrant before searching an electronic device whenever it is operating outside the border environment. Exh. 13 (CBP 30(b)(6) depo.) at 286:25–287:3, 287:7–12; Exh. 41 (CBP AMO Guidance) at Bates 1169; Exh. 42 (CBP 2017 AMCIT Memorandum) at Bates 1153.

Defendants' Response: Dispute plaintiffs' characterization of the deposition testimony and cited guidance. Further dispute that this is a material fact.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. Plaintiffs refer the Court to the cited material. This is a material fact because it is relevant to the application of the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.c.

2. ICE Obtains Warrants

110. ICE advises its agents to obtain a warrant “if time permits” and if agents have “any doubt” concerning whether a warrant is required. Exh. 43 (HSI 2012 Search and Seizure Handbook) at § 6.3, Bates 1187, § 7.11.4, Bates 1201.

Defendants' Response: Dispute this characterization. ICE advises that its agents

“operating in a non-border environment should make every effort to obtain a warrant prior to searching, even if an exception to the warrant requirement appears to exist.” *Id.* at § 8, Bates 1203. Do not dispute this statement in a non-border environment.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. Plaintiffs do not assert that this policy applies to the border environment.

111. ICE trains agents on how to seek a warrant. Exh. 14 (ICE 30(b)(6) depo.) at 251:4–7, 261:2–10. This training occurs at the ICE academy, on the job, from supervisors and senior officers, from the local U.S. Attorney’s office, and from the Office of the Principal Legal Advisor. *Id.* at 261:15–25, 262:9–16, 263:5–14, 263:24–264:15, 264:21– 265:8.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

112. ICE’s written training materials provide details on how to prepare an affidavit to establish probable cause for a warrant. Exh. 43 (HSI 2012 Search and Seizure Handbook) at § 7.11.4, Bates 1201–02, § 8.2, 1204–05.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

113. ICE policy on international mail requires:

- a. A warrant to search inbound international mail that is sealed and appears to contain only correspondence. Exh. 44 (MOU Between ICE/HSI and USPS) at § 4.A.3, Bates 1272; Exh. 14 (ICE 30(b)(6) depo.) at

248:5–9.

- b. A warrant to search outbound international mail that is sealed and weighs less than 16 ounces. Exh. 44 (MOU Between ICE/HSI and USPS) at § 4.B.3, Bates 1273.
- c. A warrant to read correspondence contained in other types of inbound and outbound international mail. *Id.* at § 4.A.2, § 4.B.2., Bates 1272–73.
- d. Reasonable suspicion of contraband to open a parcel, and a warrant to read correspondence in that parcel. *Id.* *See also* Exh. 14 (ICE 30(b)(6) depo.) at 248:10–15.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

114. If an ICE agent opens sealed mail on reasonable suspicion, and it contains correspondence on digital storage media, ICE policy requires a warrant to read that digital correspondence. Exh. 14 (ICE 30(b)(6) depo.) at 249:6–250:10.

Defendants’ Response: Dispute this characterization of ICE policy. An electronic device in the mail would not be treated as solely correspondence for purposes of a border search of mail because the electronic device is merchandise itself, regardless of the data on the device. Accordingly, the laws, regulations, and policy regarding searching sealed mail containing solely correspondence do not apply. *See* Exh. 44 at §§ 4.A.2, Bates 1272.

Plaintiffs’ Reply: Defendants’ statement that

electronic devices in the mail are merchandise is a legal assertion for which no response is required under Federal Rule of Civil Procedure 56(c) and/or Local Rule 56.1. To the extent a response is deemed required: Plaintiffs dispute, as a legal matter, Defendants' statement that all electronic devices in the mail are merchandise, and further dispute this is a material fact. However, even if the device were considered merchandise, if the device had correspondence on it, agents would stop reading and have to get a warrant to continue reading. *See* Exh. 14, ECF No. 91-13 (ICE 30(b)(6) depo.) at 249:6–250:10. Moreover, Defendants' cited evidence does not support their assertions, as the cited material is silent on the issue of whether an electronic device could both be merchandise and contain correspondence. *See* Exh. 44, ECF No. 91-43 (MOU Between ICE/HSI and USPS) at §§ 4.A.2, Bates 1272 (“Customs officers, may, without a search warrant, search inbound international mail that is sealed against inspection if a customs officer has a reasonable suspicion that the mail contains merchandise or contraband. No one acting under the authority of this section shall read or authorize any other person to read any correspondence contained in mail sealed against inspection without a search warrant”).

115. ICE agents sometimes obtain warrants at the border to conduct:

- a. X-ray searches. Exh. 14 (ICE 30(b)(6) depo.) at 259:11–16.
- b. Involuntary body cavity searches. *Id.* at

260:14–25.

- c. Detentions that last longer than eight hours. *Id.* at 254:19–255:6, 255:13– 21, 256:7–258:3.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

3. CBP and ICE Apply the Reasonable Suspicion Standard

116. Since at least 2015, CBP has had procedures for conducting advanced device searches based on reasonable suspicion. Exh. 13 (CBP 30(b)(6) depo.) at 254:7– 14; 256:9–19; Exh. 45 (CBP 2015 Memorandum on *Cotterman*) at Bates 129–30.

Defendants’ Response: No dispute that CBP has procedures for conducting advanced device searches based on reasonable suspicion of laws it enforces or administers. Dispute that this is a material fact since the Amended Complaint does not contain a claim for relief involving reasonable suspicion.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact because it is relevant to the application of the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.c. This is also a material fact because, should the Court determine that a warrant is not required, it may require reasonable suspicion. *See* Pl. Br. at Part I.C.

117. CBP officers are accustomed to applying the reasonable suspicion standard for advanced device searches. Exh. 13 (CBP 30(b)(6) depo.) at 259:8–15.

Defendants' Response: No dispute, except to dispute that this is a material fact since the Amended Complaint does not contain a claim for relief involving reasonable suspicion.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact because it is relevant to the application of the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.c. This is also a material fact because, should the Court determine that a warrant is not required, it may require reasonable suspicion. *See* Pl. Br. at Part I.C.

118. CBP has written guidance and training on reasonable suspicion. Exh. 13 (CBP 30(b)(6) depo.) at 257:11–259:7. ICE provides training to its agents on reasonable suspicion. Exh. 14 (ICE 30(b)(6) depo.) at 279:22–280:8.

Defendants' Response: No dispute, except to dispute that this is a material fact since the Amended Complaint does not contain a claim for relief involving reasonable suspicion.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact because it is relevant to the application of the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.c. This is also a material fact because, should the Court determine that a warrant is not required, it may require reasonable suspicion. *See* Pl. Br. at Part I.C.

119. ICE policy requires agents at the border to have reasonable suspicion for:

a. Strip searches. Exh. 14 (ICE 30(b)(6) depo.)

at 278:8–15. *See also* Exh. 43 (HSI 2012 Search and Seizure Handbook) at § 11.1, Bates 1224 (requiring reasonable suspicion for “partial body search[es]”).

- b. X-ray or body cavity searches. Exh. 14 (ICE 30(b)(6) depo.) at 278:18– 279:11, 279:13–20; Exh. 43 (HSI 2012 Search and Seizure Handbook) at §10.9, Bates 1219. A destructive search of a vehicle or other object. Exh. 43 (HSI 2012 Search and Seizure Handbook) at §11.1, Bates 1224.

Defendants’ Response: No dispute, except to dispute that this is a material fact since the Amended Complaint does not contain a claim for relief involving reasonable suspicion.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact because it is the application of the Fourth Amendment balancing test. *See* Pl. Br. at Part I.A.2.c. This is also a material fact because, should the Court determine that a warrant is not required, it may require reasonable suspicion. *See* Pl. Br. at Part I.C.

V. Plaintiffs’ Experiences at the Border

Defendants’ General Response: Defendants dispute that any of the facts below relating to Plaintiffs’ experiences at the border are material to the Plaintiffs’ First and Fourth Amendment facial challenges. To the extent these facts are material it would only be to their standing to bring this lawsuit.

Plaintiffs’ General Reply: The facts below

relating to Plaintiffs' experiences at the border are material to Plaintiffs' standing, and as noted are also material to Plaintiffs' First and Fourth Amendment claims.

A. Past Border Searches of Devices

1. Ghassan and Nadia Alasaad

120. Plaintiffs Ghassan and Nadia Alasaad are U.S. citizens who reside in Massachusetts and are married to each other. Exh. 1 (G. Alasaad Dec.) at ¶¶ 2–4; Exh. 2 (N. Alasaad Dec.) at ¶¶ 2–4. He works as a limousine driver, and she is a nursing student. Exh. 1 (G. Alasaad Dec.) at ¶ 1; Exh. 2 (N. Alasaad Dec.) at ¶ 1.

Defendants' Response: No dispute that Plaintiffs Ghassan and Nadia Alasaad made these statements, but dispute they are material facts.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing. *See* Pl. Br. at Part IV.

121. On January 12, 2017, they returned by car to the United States at Highgate Springs, Vermont. Exh. 1 (G. Alasaad Dec.) at ¶ 5; Exh. 2 (N. Alasaad Dec.) at ¶ 5. Ghassan Alasaad was traveling with an unlocked Samsung Note smartphone. Exh. 1 (G. Alasaad Dec.) at ¶ 5. Nadia Alasaad was traveling with a locked iPhone 7 smartphone. Exh. 2 (N. Alasaad Dec.) at ¶ 5. CBP officers conducted a manual search of Mr. Alasaad's phone. Exh. 2 (N. Alasaad Dec.) at ¶ 8; Exh. 1 (G. Alasaad Dec.) at ¶ 7; Exhs. 15 & 16 (Answer and Complaint) at ¶ 65. CBP officers later searched Ms.

Alasaad's phone. Exh. 47 (EMR) at Bates 337–38, 340.

Defendants' Response: The referenced exhibits indicate that encounter occurred on July 12, 2017, not January. Further dispute that these facts are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. Plaintiffs admit that the encounter occurred on July 12, 2017. This is a material fact to the extent that it supports Plaintiffs' standing, and the Fourth Amendment device search and confiscation claims. *See* Pl. Br. Part IV and at pp. 11, 23.

122. Nadia Alasaad objected to the search of her phone on the ground that she wears a headscarf in public in accordance with her religious beliefs, and she had photos in her phone of herself without a headscarf on and of her daughters that she did not want any CBP officers, especially male officers, to view. Exh. 2 (N. Alasaad Dec.) at ¶¶ 10, 13.

Defendants' Response: No dispute, except dispute that this fact is material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing, their First Amendment claim, and their Fourth Amendment device search claim. *See* Pl. Br. at Parts III & IV and at p. 11.

123. On August 28, 2017, Nadia Alasaad arrived at John F. Kennedy International Airport with her 11-year-old daughter. *Id.* at ¶ 19. Her daughter was traveling with a locked iPhone 6+ smartphone. *Id.* CBP officers searched Nadia Alasaad's handbag,

where they found the smartphone that her daughter was using. *Id.* at ¶ 20; Exhs. 15 & 16 (Answer and Complaint) at ¶ 74. CBP officers searched the phone. Exhs. 15 & 16 (Answer and Complaint) at ¶ 76.

Defendants’ Response: No dispute, except dispute that this fact is material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing and their Fourth Amendment device search claim. *See* Pl. Br. at Part IV and at p. 11.

2. Suhaib Allababidi

124. Plaintiff Suhaib Allababidi is a U.S. citizen who resides in Texas. Exh. 3 (Allababidi Dec.) at ¶¶ 2–3. He owns and operates a business that sells security technology. *Id.* at ¶ 1.

Defendants’ Response: No dispute that Plaintiff Allababidi made these statements in his declaration, but dispute they are material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing. *See* Pl. Br. at Part IV.

125. On January 24, 2017, Allababidi returned to Dallas, Texas, after an international trip. *Id.* at ¶ 4; Exhs. 15 & 16 (Answer and Complaint) at ¶ 77. He was traveling with a locked Samsung S7 Edge smartphone and an unlocked iPhone smartphone. Exh. 3 (Allababidi Dec.) at ¶ 4. A CBP officer seized and manually searched Allababidi’s unlocked iPhone for at least 20 minutes. *Id.* at ¶ 5. After Allababidi declined to provide the password to his locked

Samsung phone, CBP officers confiscated both phones in order to conduct an “examination.” *Id.* at ¶ 6; Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 79–80; Exh. 17 (Detention Notice and Custody Receipt) at Pls. Bates 62; *see also* Exh. 47 (Detention Notice and Custody Receipt) at Bates 107.

Defendants’ Response: Do not dispute that Plaintiff Allababidi’s phones were initially searched by CBP and then detained for further examination by an ICE Special Agent as indicated by the signature and organization listed on the cited Detention and Custody Receipt (Ex. 17). Further dispute this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing and their Fourth Amendment device search claim. *See* Pl. Br. at Part IV and at p. 11.

3. Sidd Bikkannavar

126. Sidd Bikkannavar is a U.S. citizen and a resident of California. Exh. 4 (Bikkannavar Dec.) at ¶¶ 2–3. He is an optical engineer at NASA’s Jet Propulsion Laboratory. *Id.* at ¶ 1.

Defendants’ Response: No dispute that Plaintiff Bikkannavar made these statements in his declaration, but dispute they are material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing. *See* Pl. Br. at Part IV.

127. On January 31, 2017, Bikkannavar flew into Houston, Texas, after an international trip. *Id.* at ¶ 4. He was traveling with a locked Samsung Galaxy Note 5 smartphone. *Id.* CBP officers searched Bikkannavar’s phone for 19 minutes. Exh. 47 (EMR) at Bates 621. Afterwards, a CBP officer stated they had used “algorithms” to search the phone. Exh. 4 (Bikkannavar Dec.) at ¶ 12.

Defendants’ Response: No dispute that Plaintiff Bikkannavar made these statements in his declaration, but dispute that this correctly characterizes paragraph 12 of the declaration. Further dispute that these facts are material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. Bikkannavar’s declaration at paragraph 12 states in full: “After about 30 minutes, the officer returned the phone to me and informed me that officers had used ‘algorithms’ to search the contents of the phone, which I understood to mean that they used one or more forensic tools.” Exh. 4, ECF No. 91-3 (Bikkannavar Dec.) at ¶ 12. While Defendants’ Electronic Media Report (“EMR”) states that the device search itself took 19 minutes, Exh. 47 (filed under seal) (EMR) at Bates 621, Bikkannavar testified that the phone was returned to him after about 30 minutes. This is a material fact to the extent that it supports Plaintiffs’ standing and their Fourth Amendment device search claim. *See* Pl. Br. at Part IV and at p. 11.

4. Jérémie Dupin

128. Jérémie Dupin is a lawful permanent resident who resides in Massachusetts. Exh. 5 (Dupin Dec.) at ¶ 2–3. He is a journalist. *Id.* at ¶ 1.

Defendants’ Response: No dispute that Plaintiff Dupin made these statements in his declaration but dispute they are material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing and their First Amendment claim. *See* Pl. Br. at Part III & IV.

129. On December 22, 2016, Dupin flew to Miami, Florida after an international trip. *Id.* at ¶ 4. He was traveling with a locked iPhone 5 smartphone, which he used for his journalism work. *Id.* A CBP Officer conducted a basic search of Dupin’s phone for about 15 minutes. Exhs. 15 & 16 (Answer and Complaint) at ¶ 90. *See also* Exh. 47 (EMR) at Bates 689; Exh. 5 (Dupin Dec.) at ¶ 8.

Defendants’ Response: No dispute that Plaintiff Dupin made these statements in his declaration, but dispute they are material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing, their First Amendment claim, and their Fourth Amendment device search claim. *See* Pl. Br. at Part III & IV and at p. 11.

130. On December 23, 2016, Dupin traveled by bus with his seven-year-old daughter from Montreal to New York City. He carried the same locked iPhone. Exh. 5 (Dupin Dec.) at ¶ 11. At the U.S. border

customs checkpoint, a CBP officer took the phone into another room for approximately four hours. *Id.* at ¶¶ 12–15. CBP searched it. Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 94, 96; *see also* Exh. 47 (EMR) at Bates 690–91. An officer periodically returned to ask Dupin questions about the contents of his phone. Dupin. Exh. 5 (Dupin Dec.) at ¶ 15; Exhs. 15 & 16 (Answer and Complaint) at ¶ 96.

Defendants’ Response: No dispute that Plaintiff Dupin made these statements in his declaration, but dispute they are material, but dispute that the records show that his phone was taken out of the room. See Ex.47 at Bates 711. Further dispute that these facts are material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. The records are silent as to whether Dupin’s phone was taken out of the room. Exh. 47 (filed under seal) at Bates 691, 711. However, Dupin testified to this fact in his sworn declaration. Exh. 5, ECF No. 91-4 (Dupin Dec.) at ¶ 8. This is a material fact to the extent that it supports Plaintiffs’ standing and their First Amendment claim. *See* Pl. Br. at Part III & IV.

5. Aaron Gach

131. Aaron Gach is a U.S. citizen who resides in California. Exh. 6 (Gach Dec.) at ¶¶ 2–3. He is an artist. *Id.* at ¶ 1.

Defendants’ Response: No dispute that Plaintiff Gach made these statements in his declaration but dispute they are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing. *See* Pl. Br. at Part IV.

132. On February 23, 2017, Gach arrived at San Francisco International Airport after an international trip. *Id.* at ¶ 4. Gach traveled with a locked iPhone SE smartphone. *Id.* CBP searched it. Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 102–03; Exh. 47 (EMR) at Bates 714–15.

Defendants' Response: No dispute that Plaintiff Gach made these statements in his declaration, but dispute they are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing and their Fourth Amendment device search claim. *See* Pl. Br. Part IV and at p. at 11.

6. Ismail Abdel-Rasoul aka Isma'il Kushkush

133. Isma'il Kushkush is a U.S. citizen who resides in Virginia. Exh. 7 (Kushkush Dec.) at ¶¶ 2–3. He is a freelance journalist. *Id.* at ¶ 1.

Defendants' Response: No dispute that Plaintiff Kushkush made these statements in his declaration, but dispute they are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing and their First Amendment claim. *See* Pl. Br. at

Part III & IV.

134. On March 18, 2013, Kushkush arrived at Washington Dulles International Airport after an international trip. Exh. 47 (EMR) at Bates 913. At Washington Dulles, CBP officers searched Kushkush's Blackberry Bold cell phone, two electronic storage media, and two SIM cards. *Id.* at Bates 913–14.

Defendants' Response: No dispute that Plaintiff KushKush made these statements in his declaration, but dispute they are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing and their Fourth Amendment device search claim. *See* Pl. Br. Part IV and at p. at 11.

135. On July 30, 2017, Kushkush entered the United States at Highgate Springs, Vermont, via bus from Canada. Exh. 7 (Kushkush Dec.) at ¶ 14. He was carrying a locked iPhone 7 smartphone. *Id.* CBP officers conducted a manual search of Kushkush's phone for about one hour. Exhs. 15 & 16 (Answer and Complaint) at ¶ 117. *See also* Exh. 47 (TECS records) at Bates 304, 332–33; Exh. 47 (HSI Report of Investigation) at Bates 105.

Defendants' Response: No dispute that Plaintiff KushKush made these statements in his declaration, but dispute they are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing and their Fourth Amendment device search claim.

See Pl. Br. at Part IV and at p. 11.

7. Zainab Merchant

136. Zainab Merchant is a U.S. citizen who resides in Toronto, Canada. Exh. 8 (Merchant Dec.) at ¶¶ 2–3. She is a writer, graduate student, and the founder and editor of a media website. *Id.* at ¶ 1.

Defendants’ Response: No dispute that Plaintiff Merchant made these statements in her declaration, but dispute they are material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing. *See* Pl. Br. at Part IV.

137. On March 5, 2017, Merchant arrived at the Toronto airport for a flight to Orlando. *Id.* at ¶ 4. She traveled with a locked Samsung smartphone. *Id.* CBP searched Merchant’s phone. Exhs. 15 & 16 (Answer and Complaint) at ¶ 135. *See also* Exh. 47 (EMR) at Bates 754. The search lasted 25 minutes. Exh. 47 (EMR) at Bates 754.

Defendants’ Response: No dispute that Plaintiff Merchant made these statements in her declaration, but dispute they are material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing and their Fourth Amendment device search claim. *See* Pl. Br. at Part IV and at p. 11.

138. CBP officers questioned her about her religious affiliation and her blog, including asking her about an article she had written on the blog that

described a previous border crossing experience. Exh. 8 (Merchant Dec.) at ¶ 11.

Defendants' Response: No dispute that Plaintiff Merchant made this statement in her declaration, but dispute it accurately characterizes the encounter and refer the Court to Ex. 47, Bates 766. Further dispute this fact is material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. The records Defendants cite are silent as to whether CBP officers questioned Merchant about her religious affiliation and her blog. Exh. 47 (filed under seal) at Bates 766. However, Merchant has testified to these facts in her sworn declaration. Exh. 8, ECF No. 91-7 (Merchant Dec.) at ¶ 11. This is a material fact to the extent that it supports Plaintiffs' standing. *See* Pl. Br. at Part IV.

139. Merchant was concerned about CBP officers searching her phone because she wears a headscarf in public in accordance with her religious beliefs, and the phone contained pictures of her without her headscarf that she did not want officers to see. *Id.* at ¶ 6.

Defendants' Response: No dispute that Plaintiff Merchant expressed this concern in her declaration but dispute that the statement accurately characterize the encounter and refer the Court to Ex. 47, Bates 766. This concern appears to have been expressed in the search conducted on July 7, 2018. *See* Ex. 47. Bates 757. Further dispute this fact is material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. The fact discusses why

Merchant did not want her phone searched rather than if she communicated this information to CBP officers. Exh. 8, ECF No. 91-7 (Merchant Dec.) at ¶ 11. This is a material fact to the extent that it supports Plaintiffs' standing, their First Amendment claim, and their Fourth Amendment device search claim. See Pl. Br. at Part III & IV and at p. 11.

140. On April 5, 2018, Merchant arrived in Orlando, Florida, after an international trip. Exh. 8 (Merchant Dec.) at ¶ 14. She carried a locked Samsung Note 8 smartphone. *Id.* CBP officers searched it. Exh. 47 (EMR) at Bates 908.

Defendants' Response: No dispute, except dispute that these facts are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing and their Fourth Amendment device search claim. See Pl. Br. at Part IV and at p. 11.

141. On July 7, 2018, Merchant arrived in Fort Lauderdale, Florida, after an international trip. Exh. 8 (Merchant Dec.) at ¶ 22. She carried a locked Samsung Note 8 smartphone. *Id.* A CBP officer searched Merchant's phone for about 15 minutes. Exh. 47 (EMR) at Bates 755, 758.

Defendants' Response: No dispute, except dispute that these facts are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing and their Fourth Amendment device search claim.

See Pl. Br. at Part IV and at p. 11.

142. On September 9, 2018, Merchant traveled from Toronto, Ontario, to Orlando, Florida. Exh. 8 (Merchant Dec.) at ¶ 27. She carried a locked Samsung Note 8 smartphone. *Id.* A CBP officer directed Merchant to turn over her smartphone. Merchant told the officer that she did not consent to the search and that her device contained attorney-client privileged communications. *Id.* at ¶ 28. Nonetheless, “CBP conducted a basic search of Ms. Merchant’s cell phone,” which lasted about ten minutes. Exh. 24 (Email from Marsha Edney, Sept. 20, 2018). *See also* Exh. 47 (EMR) at Bates 759–60. Merchant saw the officer viewing emails and text messages between herself and her lawyer. Exh. 8 (Merchant Dec.) at ¶ 31.

Defendants’ Response: No dispute except to dispute that the third and last sentences accurately characterize the encounter and refer the Court to Ex. 47, Bates 757-58 for an accurate description. Further dispute these facts are material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. Defendants’ citation to Exh. 47 (filed under seal) at Bates 757–58, relates to the July 7, 2018 border device search, and not the September 9, 2018 border device search. This is a material fact to the extent that it supports Plaintiffs’ standing, their First Amendment claim, and their Fourth Amendment device search claim. *See* Pl. Br. at Part III & IV and at p. 11.

8. Akram Shibly

143. Mohammed Akram Shibly is a U.S. citizen who currently lives in Los Angeles. Exh. 9 (Shibly Dec.) at ¶¶ 2–3. He is a filmmaker and a graduate student. *Id.* at ¶ 1.

Defendants’ Response: No dispute that Plaintiff Shibly made these statements in his declaration, but dispute they are material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing. *See* Pl. Br. at Part IV.

144. On January 1, 2017, Shibly entered the United States at the Lewiston- Queenston Bridge in New York. *Id.* at ¶ 4. He was carrying a locked iPhone 6+ smartphone. *Id.* A CBP officer searched it. Exhs. 15 & 16 (Answer and Complaint) at ¶ 140. *See also* Exh. 47 (EMR) at Bates 847, 849. The search lasted 37 minutes. Exh. 47 (EMR) at Bates 847.

Defendants’ Response: No dispute, except dispute that the facts are material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing and their Fourth Amendment device search claim. *See* Pl. Br. at Part IV and at p. 11.

9. Matthew Wright

145. Matthew Wright is a U.S. citizen who resides in Colorado. Exh. 10 (Wright Dec.) at ¶¶ 2–3. He is a computer programmer. *Id.* at ¶ 1.

Defendants’ Response: No dispute that Plaintiff Wright made these statements in his

declaration, but dispute they are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing. *See* Pl. Br. at Part IV.

146. On April 21, 2016, Wright arrived in Denver, Colorado, after an international trip. *Id.* at ¶ 5. Wright was traveling with a locked iPhone 6 smartphone, a locked MacBook Pro laptop, and an unlocked GoPro camera. *Id.* Wright declined a CBP officer's demand to unlock his laptop. As a result, CBP officers confiscated his laptop, phone, and camera. *Id.* at ¶ 6.

Defendants' Response: No dispute, except dispute that they are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing and their Fourth Amendment device search claim. *See* Pl. Br. at Part IV and at p. 11.

147. "CBP extracted and obtained information from Plaintiff Wright's devices." Exhs. 15 & 16 (Answer and Complaint) at ¶ 155. Specifically, an ICE agent "attempted to image Mr. Wright's laptop with MacQuisition software, and a CBP forensic scientist extracted data from the SIM card in Wright's phone and from his camera." Exhs. 15 & 16 (Answer and Complaint) at ¶ 44. *See also* Exh. 25 (June 6, 2016 CBP email) at Pls. Bates 953; Exh. 47 (HSI Digital Forensic Report) Bates 98.

Defendants' Response: No dispute, except dispute that they are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing. *See* Pl. Br. at Part IV.

10. Diane Maye Zorri

148. Diane Maye Zorri is a U.S. citizen who resides in Florida. Exh. 11 (Zorri Dec.) at ¶¶ 2–3. She is a university professor and a former United States Air Force captain. *Id.* at ¶ 1.

Defendants' Response: No dispute that Plaintiff Zorri made these statements in her declaration, but dispute they are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing. *See* Pl. Br. at Part IV.

149. On June 25, 2017, Zorri arrived in Miami, Florida, after an international trip. *Id.* at ¶ 4. Zorri was traveling with a MacBook Pro laptop and an iPhone 7 smartphone, both locked. *Id.* CBP searched Zorri's phone for about 45 minutes. Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 121, 124. *See also* Exh. 47 (EMR) at Bates 729, 731.

Defendants' Response: No dispute that Plaintiff Zorri made these statements in her declaration but Defendants note that the referenced EMR pages (729-731) only mention an iPhone. Further dispute these facts are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. The Electronic Media Report specifically mentions Maye Zorri's "Apple cell phone." Exh. 47 (filed under seal) (TECS records) at 729. Maye Zorri also testified to both her cell phone and laptop being searched. Exh. 11, ECF No. 91-10 (Maye Zorri Decl.) at ¶¶ 5–8. Additionally, the EMR states that "All of the electronic *devices* were returned to the traveler." Exh. 47 (filed under seal) (TECS records) at Bates 731 (emphasis added). This is a material fact to the extent that it supports Plaintiffs' standing and their Fourth Amendment device search claim. *See* Pl. Br. at Part IV and at p. 11.

B. Ongoing Retention of Information From Past Device Searches

150. Defendants have retained in TECS information its officers observed during the search of the contents of seven Plaintiffs' phones: Ghassan Alasaad, Nadia Alasaad, Bikkannavar, Dupin, Merchant, Shibly, and Zorri. Exh. 26 (Defs. Interrog. Responses) at #10 (Nadia Alasaad, Bikkannavar, Dupin, Merchant, and Zorri); Exh. 47 (TECS records) at Bates 340, 351, 355, 359 (Ghassan Alasaad); Exh. 47 (TECS records) at Bates 340, 351, 355, 359 (Nadia Alasaad); Exh 47 (TECS records) at Bates 691, 711 (Dupin); Exh 47 (TECS records) at Bates 849, 873, 878 (Shibly).

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

151. Defendants also have retained information copied from Wright's electronic devices.

- a. The data extracted from Wright's devices was stored on three thumb drives. Exh. 25 (EMR) at Pls. Bates 938.

Defendants' Response: No dispute.

Plaintiffs' Reply: No dispute.

- b. Two months after CBP returned Wright's devices to him, CBP continued to retain the thumb drives. Exh. 47 (EMR) at Bates 888; Exh. 47 (log of items received by CBP laboratory) at Bates 909; Exh. 28 (Def. Privilege Log of 12/7/18) (describing Bates 909 as "[l]og of items received by CBP laboratory"); Exh. 24 (Email from Marsha Edney, Nov. 21, 2018) (describing Bates 909 as "a log of items received by a law enforcement laboratory, and includes a notation of receipt of thumb drives relating to the inspection of Plaintiff Wright's electronic devices").

Defendants' Response: Dispute that these facts are material and the inference being drawn by the absence of a document showing destruction. Defendants aver that all copies of Wright's data have been deleted. *See* Declaration of Jenny Tsang (Ex. L.). There is no material dispute because this information is uniquely within Defendants' knowledge and does not matter as a matter of law.

Plaintiffs' Reply: No dispute.

- c. DHS policy requires that "a record of the destruction [of information from a traveler's device] is documented in the TECS Report of

Investigation (ROI).” Exh. 29 (DHS 2009 PIA), at Bates 228. In both civil discovery in this case and in response to a FOIA request from Wright, CBP and ICE produced no records showing that the data retained on the thumb drives was destroyed. Exh. 12 (Cope Dec.) at ¶¶ 4–5.

Defendants’ Response: No dispute.

Plaintiffs’ Reply: No dispute.

C. Past Device Confiscations¹

1. Ghassan and Nadia Alasaad

152. CBP officers retained Ghassan and Nadia Alasaad’s phones after the Alasaads left the border area on July 12, 2017. Exh. 1 (G. Alasaad Dec.) at ¶ 15; Exh. 47 (EMR) at Bates 340.

Defendants’ Response: Dispute only to the extent that that the undefined term “retained” is used. Admit that the phones were detained. Ex. 47 at Bates 340.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. Plaintiffs use the term “retained” as a synonym for detained or confiscated.

153. Ghassan and Nadia Alasaad had to spend approximately \$1,000 to purchase two new phones. Exh. 1 (G. Alasaad Dec.) at ¶ 17; Exh. 2 (N. Alasaad

¹ Defendants disagree with the use of the term “confiscations” but admit that they do sometimes detain and/or seize electronic devices.

Dec.) at ¶ 17.

Defendants' Response: No dispute that Plaintiffs Ghassan and Nadia Alasaad made this statement in their declarations, but dispute that the fact is material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing. *See* Pl. Br. at Part IV.

154. Twelve days after Ghassan and Nadia Alasaad crossed the border, CBP officials sent their phones back to them. Exhs. 15 & 16 (Answer and Complaint) at ¶ 72.

Defendants' Response: No dispute, except dispute that it is material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing and their Fourth Amendment device confiscation claim. *See* Pl. Br. at Part IV and at p. 23.

155. Soon after receiving his phone from CBP, Ghassan Alasaad attempted to access certain media files in his WhatsApp application, including videos of his daughter's graduation. The phone displayed the message, "Sorry, this media file doesn't exist on your internal storage." This did not occur prior to CBP's confiscation of the phone. Exh. 1 (G. Alasaad Dec.) at ¶ 19.

Defendants' Response: No dispute that Plaintiff Alasaad made these statements in his declaration, but Defendants lack knowledge or information to determine if they are true or not.

Further, dispute that the facts are material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing. *See* Pl. Br. at Part IV.

2. Suhaib Allababidi

156. On January 24, 2017, CBP officers detained Allababidi's unlocked iPhone and locked Samsung smartphone after he had been permitted to leave the border area. Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 79–80; Exh. 3 (Allababidi Dec.) at ¶ 6.

Defendants' Response: No dispute, except dispute that it is material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing. *See* Pl. Br. at Part IV.

157. CBP officers confiscated Allababidi's unlocked phone even though an officer had already manually searched the phone and returned it to Allababidi. Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 79–80; Exh. 3 (Allababidi Dec.) at ¶¶ 5–6.

Defendants' Response: Dispute only to the extent that the undefined term confiscate is used. Further dispute that this is material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing. *See* Pl. Br. at Part IV.

158. Allababidi had to spend more than \$1,000 on

replacement phones. Exh. 3 (Allababidi Dec.) at ¶ 9.

Defendants’ Response: No dispute that Plaintiff Allababidi made this statement in his declaration, but dispute that the fact is material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing. *See* Pl. Br. at Part IV.

159. Allababidi’s phones were sent to the “Regional Computer Forensic Lab” on February 15, 2017, and then sent to another location on March 3, 2017. Exh. 47 (Detention Notice and Custody Receipt) at Bates 107.

Defendants’ Response: No dispute, except dispute that it is material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing. *See* Pl. Br. at Part IV.

160. The unlocked iPhone was returned to Allababidi more than two months after confiscation. Exh. 3 (Allababidi Dec.) at ¶ 7. *See also* Exh. 47 (Detention Notice and Custody Receipt) at Bates 107.

Defendants’ Response: No dispute, except dispute that it is material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing and their Fourth Amendment device confiscation claim. *See* Pl. Br. at Part IV and at p. 23.

161. The locked Samsung smartphone was returned to Allababidi on December 13, 2017, more than ten months after confiscation, and just two days before Defendants moved to dismiss in this case. Exh. 3 (Allababidi Dec.) at ¶ 8; Exh. 32 (Def. Motion to Dismiss) at p. 9.

Defendants’ Response: No dispute, except dispute that it is material.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs’ standing and their Fourth Amendment device confiscation claim. *See* Pl. Br. at Part IV and at p. 23.

3. Matthew Wright

162. CBP officers seized Wright’s smartphone, laptop, and GoPro camera on April 21, 2016. Exh. 25 (Detention Notice and Custody Receipt) at Pls. Bates 945.

Defendants’ Response: Dispute only to the extent that that the term “seized” is used. Admit that the devices were detained. Ex. 25 at Bates 945.

Plaintiffs’ Reply: Defendants do not raise a genuine dispute. Plaintiffs use the term “seized” as a synonym for detained or confiscated.

163. An officer informed Wright that it might take CBP as long as a year to return his devices to him. Exh. 10 (Wright Dec.) at ¶ 7.

Defendants’ Response: No dispute that Plaintiff Wright states this in his declaration,

but dispute that his is a material fact.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing. *See* Pl. Br. at Part IV.

164. Wright spent \$2,419.97 for a new laptop and phone. Exh. 10 (Wright Dec.) at ¶ 8. As a computer programmer, Wright's livelihood depends on these tools. *Id.*

Defendants' Response: No dispute that Plaintiff Wright states this in his declaration, but Defendants lack any knowledge of these facts. Further dispute these are material facts.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing. *See* Pl. Br. at Part IV.

165. Wright's electronic devices were transferred between CBP and ICE facilities multiple times. Exh. 25 (EMR) at Pls. Bates 936–38.

Defendants' Response: No dispute, except dispute that it is material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing. *See* Pl. Br. at Part IV.

166. CBP returned Wright's electronic devices to him after 56 days, on June 16, 2016. Exh. 25 (EMR) at Pls. Bates 938; Exh. 10 (Wright Dec.) at ¶ 9.

Defendants' Response: No dispute, except dispute that it is material.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. This is a material fact to the extent that it supports Plaintiffs' standing and their Fourth Amendment device confiscation claim. *See* Pl. Br. at Part IV and at p. 23.

D. Other Recurring Border Scrutiny

167. Eight Plaintiffs have been subjected to recurring secondary inspections during border crossings. Exh. 47 (TECS records) at Bates 338, 348, 350–51, 362–367 (six of Ghassan Alasaad); Exh. 47 (TECS records) at Bates 338, 350, 363–64 (three of Nadia Alasaad); Exh. 47 (TECS records) at Bates 586–88, 590, 592–95, 600, 602–04, 606, 608–620 (nine of Allababidi); Exh. 47 (TECS records) at Bates 678, 680–82, 684–85, 688 (seven of Bikkannavar); Exh. 47 (TECS records) at Bates 704–05, 707–13 (six of Dupin); Exh. 47 (TECS records) at Bates 319–322, 324–25, 327, 329–30, 332–35, 913–15 (eight of Kushkush); Exh. 47 (TECS records) at Bates 817, 819–22, 824–26, 828–30, 832, 834, 836–39, 841–45 (eight of Merchant); Exh. 47 (TECS records) at Bates 868, 870, 880, 884–85 (four of Shibly).

Defendants' Response: Do not dispute that these Plaintiffs have been referred to secondary inspections on multiple occasions but dispute that the cited TECS records for Nadia Alasaad and Bikkannavar indicate that they were searched 3 or 7 times, respectively. Further dispute that this is a material fact.

Plaintiffs' Reply: Defendants do not raise a genuine dispute. TECS records indicate that Nadia Alasaad was subject to three secondary

inspections. *See* Exh. 47 (filed under seal) at Bates 338, 350 (July 13, 2017); Bates 363–64 (Feb. 27, 2014); Exh. 48 (filed under seal) at Bates 360 (Aug. 17, 2015). TECS records indicate that Bikkannavar was subject to seven secondary inspections. Exh. 48 (filed under seal) at Bates 668, 670 (Aug. 27, 2014); Bates 672 (Aug. 4, 2015); Bates 674, 676 (Jan. 2, 2016); Bates 686 (Jan. 4, 2004); Bates 687 (July 22, 2005); Exh. 47 (filed under seal) at Bates 678, 680–82, 684–85 (Jan. 31, 2017); Bates 688 (Oct. 10, 2008). This is a material fact to the extent that it supports Plaintiffs’ standing. *See* Pl. Br. at Part IV.

168. Seven Plaintiffs are subjected to recurring bag searches at the border. Exh. 47 (TECS records) at Bates 348, 365–66 (three of Ghassan Alasaad); Exh. 47 (TECS records) at Bates 348, 910–11 (two of Nadia Alasaad); Exh. 47 (TECS records) at Bates 395–96, 593, 602–03 (three of Allababidi in 2017 alone); Exh. 47 (TECS records) at Bates 709–10, 713 (three of Dupin); Exh. 47 (TECS records) at Bates 299, 306, 915 (three of Kushkush); Exh. 47 (TECS records) at Bates 766, 824–26, 828, 830, 832, 838–39, 843, 845 (six of Merchant); Exh. 47 (TECS records) at Bates 868, 875, 880 (three of Shibly).

Defendants’ Response: Do not dispute that these Plaintiffs have been subject to at least one bag search at the border but dispute that the cited TECS records for Ghassan Alasaad, Nadia Alasaad and Dupin indicate that their bags were searched 3, 2 and 3 times respectively. Further dispute that this is a material fact.

Plaintiffs’ Reply: Defendants do not raise a

genuine dispute. TECS records indicate that Ghassan Alasaad was subject to three bag searches. *See* Exh. 47 (filed under seal) at Bates 348 (July, 12, 2017); Bates 365 (Sept. 7, 2006); Bates 366 (Dec. 12, 2005). TECS records indicate that Nadia Alasaad was subject to at least one bag search. *See id.* at Bates 910–11 (Aug. 28, 2017). TECS records indicate that Dupin was subject to three bag searches. *See id.* at Bates 709 (Dec. 22, 2016); Bates 710 (Dec. 23, 2016); Bates 713 (March 6, 2017). This is a material fact to the extent that it supports Plaintiffs’ standing. *See* Pl. Br. at Part IV.

E. Regular International Travel, Past and Future

1. Ghassan and Nadia Alasaad

169. Ghassan Alasaad has returned to the United States from an international trip at least 13 times since January 1, 2013. Exh. 1 (G. Alasaad Dec.) at ¶ 22. Nadia Alasaad has done so at least 15 times during this period. Exh. 2 (N. Alasaad Dec.) at ¶ 27.

Defendants’ Response: No dispute that Plaintiffs Ghassan and Nadia Alasaad made these statements in their declarations.

Plaintiffs’ Reply: No dispute.

170. Ghassan and Nadia Alasaad intend to continue traveling internationally for personal reasons, and will carry electronic devices with them when they do so. Exh. 2 (N. Alasaad Dec.) at ¶¶ 26, 28; Exh. 1 (G. Alasaad Dec.) at ¶¶ 21, 23. For example, in the summer of 2019, they intend to travel to Egypt, Jordan, and/or Turkey. Exh. 1 (G. Alasaad Dec.) at ¶ 24; Exh. 2 (N. Alasaad Dec.) at ¶ 29. Likewise, during

the summer of 2019, Nadia Alasaad may travel to Canada. Exh. 2 (N. Alasaad Dec.) at ¶ 30.

Defendants' Response: No dispute that Plaintiffs Ghassan and Nadia Alasaad made these statements in their declarations but Defendants lack knowledge of their future travel plans.

Plaintiffs' Reply: No dispute.

2. Suhaib Allababidi

171. Allababidi has returned to the United States from an international trip at least seven times since January 1, 2013. Exh. 3 (Allababidi Dec.) at ¶ 12.

Defendants' Response: No dispute that Plaintiff Allababidi made this statement in his declaration.

Plaintiffs' Reply: No dispute.

172. Allababidi intends to continue traveling internationally for business and personal reasons, and will carry electronic devices with him when he does so. *Id.* at ¶¶ 11, 13. For example, he has reserved flights to Turkey in May and home in July of this year, and he may visit China later this year. *Id.* at ¶¶ 14–15.

Defendants' Response: No dispute that Plaintiff Allababidi made this statement in his declaration but Defendants lack knowledge of his future travel plans.

Plaintiffs' Reply: No dispute.

3. Sidd Bikkannavar

173. Bikkannavar has returned to the United States from an international trip at least 36 times

since January 1, 2013. Exh. 4 (Bikkannavar Dec.) at ¶ 17.

Defendants' Response: No dispute that Plaintiff Allababidi made this statement in his declaration.

Plaintiffs' Reply: No dispute.

174. Bikkannavar intends to continue traveling internationally for personal reasons, and will carry electronic devices with him when he does so. Exh. 4 (Bikkannavar Dec.) at ¶¶ 16, 18. For example, he plans to take eight international trips by September 2020 to participate in solar car races and related activities. *Id.* at ¶ 19.

Defendants' Response: No dispute that Plaintiff Bikkannavar made this statement in his declaration but Defendants lack knowledge of his future travel plans.

Plaintiffs' Reply: No dispute.

4. Jérémie Dupin

175. Dupin has returned to the United States from an international trip at least 21 times since January 1, 2013. Exh. 5 (Dupin Dec.) at ¶ 19.

Defendants' Response: No dispute that Plaintiff Dupin made this statement in his declaration.

Plaintiffs' Reply: No dispute.

176. Dupin intends to continue traveling internationally for business and personal reasons, and will carry electronic devices with him when he does so. *Id.* at ¶¶ 18, 20. For example, he intends to visit his daughter in Canada. *Id.* at ¶ 21. Also, as a journalist,

he intends to travel to Haiti in May or June of 2019, and he may travel to Venezuela later this year. *Id.* at ¶ 22.

Defendants' Response: No dispute that Plaintiff Dupin made this statement in his declaration but Defendants lack knowledge of his future travel plans.

Plaintiffs' Reply: No dispute.

5. Aaron Gach

177. Gach has returned to the United States from an international trip at least seven times since January 1, 2013. Exh. 6 (Gach Dec.) at ¶ 14.

Defendants' Response: No dispute that Plaintiff Gach made this statement in his declaration.

Plaintiffs' Reply: No dispute.

178. Gach intends to continue traveling internationally for business and personal reasons, and will carry electronic devices with him when he does so. *Id.* at ¶¶ 13, 15. For example, he has purchased airline tickets to Germany in June and home in July. *Id.* at ¶ 16.

Defendants' Response: No dispute that Plaintiff Gach made this statement in his declaration but Defendants lack knowledge of his future travel plans.

Plaintiffs' Reply: No dispute.

6. Isma'il Kushkush

179. Kushkush has returned to the United States from an international trip at least eight times since

January 1, 2013. Exh. 7 (Kushkush Dec.) at ¶ 22.

Defendants' Response: No dispute that Plaintiff KushKush made this statement in his declaration.

Plaintiffs' Reply: No dispute.

180. Kushkush intends to continue traveling internationally for his journalism and for personal reasons, and will carry electronic devices with him when he does so. *Id.* at ¶¶ 21, 23.

Defendants' Response: No dispute that Plaintiff KushKush made this statement in his declaration but Defendants lack knowledge of his future travel plans.

Plaintiffs' Reply: No dispute.

7. Zainab Merchant

181. Merchant has returned to the United States from an international trip at least 12 times since January 1, 2013. Exh. 8 (Merchant Dec.) at ¶ 35.

Defendants' Response: No dispute that Plaintiff Merchant made this statement in her declaration.

Plaintiffs' Reply: No dispute.

182. Merchant intends to continue traveling internationally for professional and personal reasons, and will carry electronic devices with her when she does so. *Id.* at ¶¶ 34, 36. For example, from now through May 2020, she plans to periodically travel from her current residence in Canada to her university in Boston in order to complete graduate studies. *Id.* at ¶ 37.

Defendants' Response: No dispute that Plaintiff Merchant made this statement in her declaration but Defendants lack knowledge of her future travel plans.

Plaintiffs' Reply: No dispute.

8. Akram Shibly

183. Shibly has returned to the United States from an international trip at least 18 times since January 1, 2013. Exh. 9 (Shibly Dec.) at ¶ 18.

Defendants' Response: No dispute that Plaintiff Shibly made this statement in his declaration.

Plaintiffs' Reply: No dispute.

184. Shibly plans to continue traveling internationally for business and personal reasons, and will carry electronic devices with him when he does so. *Id.* at ¶¶ 17, 19.

Defendants' Response: No dispute that Plaintiff Shibly made this statement in his declaration but Defendants lack knowledge of his future travel plans.

Plaintiffs' Reply: No dispute.

9. Matthew Wright

185. Wright has returned to the United States from an international trip at least 22 times since January 1, 2013. Exh. 10 (Wright Dec.) at ¶ 16.

Defendants' Response: No dispute that Plaintiff Wright made this statement in his declaration.

Plaintiffs' Reply: No dispute.

186. Wright plans to continue traveling internationally for personal reasons, and will carry electronic devices with him when he does so. *Id.* at ¶¶ 15, 17.

Defendants' Response: No dispute that Plaintiff Wright made these statements in his declaration, but Defendants lack knowledge of his future travel plans.

Plaintiffs' Reply: No dispute.

187. Wright attends ultimate Frisbee tournaments outside the United States regularly, and has attended a tournament in Portugal in June or July each year for the past five years. Wright's brother lives in Scotland, and it is common for him to take at least one trip a year to visit him there or elsewhere in Europe. Wright also has a group of friends who enjoy travel and Wright typically plans a trip or two abroad each year. *Id.* at ¶ 17. Wright has booked plane tickets for one international trip from June 24, 2019 through July 1, 2019. *Id.* at ¶ 18.

Defendants' Response: No dispute that Plaintiff Wright made these statements in his declaration but Defendants lack knowledge of his future travel plans.

Plaintiffs' Reply: No dispute.

10. Diane Maye Zorri

188. Zorri has returned to the United States from an international trip at least 10 times since January 1, 2013. Exh. 11 (Zorri Dec.) at ¶ 11.

Defendants' Response: No dispute that

Plaintiff Zorri makes this statement in her declaration.

Plaintiffs' Reply: No dispute.

189. Zorri plans to continue traveling internationally for professional and personal reasons, and will carry electronic devices with her when she does so. *Id.* at ¶¶ 10, 12. For example, it is significantly possible that Zorri will travel to Italy in June or July 2019, and Zorri has tentative plans to attend conferences in Europe in June and November 2019. *Id.* at ¶¶ 13–14.

Defendants' Response: No dispute that Plaintiff Zorri makes this statement in her declaration but Defendants lack knowledge of her future travel plans.

Plaintiffs' Reply: No dispute.

Respectfully submitted:

Dated: July 3, 2019

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

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

/s/ Esha Bhandari
Esha Bhandari*
Hugh Handeyside*
Nathan Freed Wessler*
AMERICAN CIVIL
LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th
Floor
New York, NY 10004
(212) 549-2500 (phone)
(212) 549-2583 (fax)
ebhandari@aclu.org
hhandeyside@aclu.org
nwessler@aclu.org

**Admitted pro hac vice
Counsel for Plaintiffs*

CERTIFICATE OF SERVICE

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

/s/ Esha Bhandari

Esha Bhandari

APPENDIX G

HOMELAND SECURITY INVESTIGATIONS

Message from the AD of Domestic Operations

May 11, 2018

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

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 1400-0SC.

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 605 1D.

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

APPENDIX I

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.

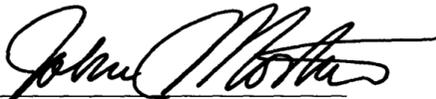
- 3) Sharing. Information that is determined to be protected by law as privileged or sensitive is to be handled consistent with the laws and policies governing such information.

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

APPENDIX J

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

No. 17-cv-11730-DJC

GHASSAN ALASAAD, et al.,

Plaintiffs,

v.

ALEJANDRO N. MAYORKAS, Secretary of the U.S.
Department of Homeland Security, in his official
capacity, TROY MILLER, Senior Official Performing
the Duties of the Commissioner of U.S. Customs and
Border Protection, in his official capacity, and TAE
D. JOHNSON, Acting Director, U.S. Immigration
and Customs Enforcement, in his official capacity.

Defendants.

Hon. DENISE J. CASPER

April 21, 2021

FINAL JUDGMENT

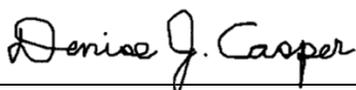
Pursuant to Federal Rule of Civil Procedure 58, the
Opinion of the Court of Appeals for the First Circuit,
ECF No. 123, the Judgment of the Court of Appeals
for the First Circuit, ECF No. 124, and the Mandate
of the Court of Appeals for the First Circuit, ECF No.
125,

IT IS HEREBY ORDERED, ADJUDGED, AND

DECREED that,

1. Judgment is entered for Defendants;
2. All Declaratory and Injunctive relief previously ordered by the Court, ECF No. 112, is vacated.

SO ORDERED.

A handwritten signature in black ink that reads "Denise J. Casper". The signature is written in a cursive style with a large, looped 'D' and 'C'. Below the signature is a solid horizontal line.

Denise J. Casper
United States District Court Judge