UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

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

MEMORANDUM AND ORDER

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

I. Introduction

Plaintiffs Ghassan Alasaad, Nadia Alasaad, Suhaib Allababidi, Sidd Bikkannavar, Jérémie Dupin, Aaron Gach, Ismail Abdel-Rasoul a/k/a Isma'il Kushkush, Diane Maye, Zainab Merchant, Mohammed Akram Shibly and Matthew Wright (individually, by last name and collectively, "Plaintiffs") bring this suit against the following persons in their official capacities: Kirstjen

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

II. Standard of Review

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

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

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

III. Factual Summary

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

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

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

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

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

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

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

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

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

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

IV. Procedural History

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

V. Discussion

A. Standing

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

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

1. Standing to Seek Injunctive or Declaratory Relief

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

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

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

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

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

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

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

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

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

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

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

2. Standing to Seek Expungement

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

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

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

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

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

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

B. Plaintiffs' Fourth Amendment Claim (Count I)

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

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

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

1. Border Search Exception to the Warrant Requirement

The border search exception, "grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country," is one such exception. United States v. Ramsey, 431 U.S. 606, 620 (1977). As previously observed by this Court:

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

> explaining that customs officers "are also charged . . . with protecting this Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics, or explosives." Montoya de Hernandez, 473 U.S. at 544.

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

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

2. Governmental Interests at the Border Are Paramount

Defendants have a paramount interest in maintaining "territorial integrity" at the border. They define such interest to include the responsibility to "ensure the interdiction of persons and goods illegally entering or exiting the United States;" "facilitate and expedite the flow of legitimate

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

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

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

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

3. Even Border Searches Are Not Boundless

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

opinion that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: [a] phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." Id. at 396-397 (emphasis in original). Riley, thus shows the challenge of applying and extending precedent concerning searches to new technology that presents a new privacy paradigm. See Carpenter v. United States, __ U.S.__, 138 S. Ct. 2206, 2222 (2018) (citing Riley, 573 U.S. at 386, ruling that the government must generally obtain a warrant to access cell phone location information and noting "[w]hen confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents"); United States v. Davis, 785 F.3d 498, 520 (11th Cir. 2015) (noting that "[j]udges cannot readily understand how . . . technologies may develop, cannot easily appreciate context, and often cannot even recognize whether the facts of the case before them raise privacy implications that happen to be typical or atypical") (citing Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L.Rev. 801, 858–59 (2004)); Morgan v. Fairfield Cty., Ohio, 903 F.3d 553, 575 n. 3 (6th Cir. 2018) (noting "how ever-changing technology fits within the contours of these zones may continue to challenge courts"). Riley also shows the vast privacy interests against which the promotion of governmental interests must be weighed.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Plaintiffs' First Amendment Claim (Count II)

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

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

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

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

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

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

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

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

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

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

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

E. Relief Sought

1. Expungement Not Warranted Here

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

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

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

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

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

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

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

2. Extent of Declaratory and Injunctive Relief

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

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

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

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

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

VI. Conclusion

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

So Ordered.

/s/ Denise J. Casper
United States District Judge