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, 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. **May 9, 2018**

I. Introduction

Plaintiffs Ghassan Alasaad, Nadia Alasaad, Suhaib Allababidi ("Allababidi"), Sidd Bikkannavar ("Bikkannavar"), Jérémie Dupin ("Dupin"), Aaron Gach ("Gach"), Ismail Abdel-Rasoul a/k/a Isma'il Kushkush ("Kushkush"), Diane Maye ("Maye"), Zainab Merchant ("Merchant"), Mohammed Akram Shibly ("Shibly") and Matthew Wright ("Wright")

(collectively, "Plaintiffs") bring this suit against the following persons in their official capacities: Kirstjen Nielsen ("Nielsen"), Secretary of the U.S. Department of Homeland Security ("DHS"),[1] Kevin McAleenan ("McAleenan"), Acting Commissioner of U.S. Customs and Border Protection ("CBP"), and Thomas Homan ("Homan"), Acting Director of U.S. Immigration and Customs Enforcement ("ICE") (collectively, "Defendants"). D. 7 ¶¶ 14-26. Plaintiffs, ten U.S. citizens and one lawful permanent resident, allege that Defendants' conduct—searching Plaintiffs' electronic devices at ports of entry to the United States and, in some instances, confiscating the electronic devices being searched, pursuant to CBP and ICE policies—violates the Fourth Amendment (Counts I and III) and First Amendment (Count II) of the U.S. Constitution. D. 7 ¶¶ 1-10, 168-73. They seek declaratory and injunctive relief. D. 7 at 40-42. Defendants have now moved to dismiss. D. 14. For the reasons stated below, the Court DENIES Defendants' motion to dismiss.

II. Standard of Review

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

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

III. Factual Background

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

In the United States, ninety-five percent of adults own a cell phone, seventy-seven percent own a smart phone and over fifty percent own a tablet computer. D. 7 ¶ 27. "Electronic devices are often essential to people's work," as well as "communication . . . navigation, shopping, banking, entertainment, news, and photography, among other functions." D. 7 ¶¶ 36, 27. "Laptops sold in 2017 can store up to two terabytes" of data, tablet computers can hold up to a terabyte and "smartphones can store hundreds of gigabytes of data." D. 7 ¶ 30. This storage capacity "can be the equivalent of hours of video files, thousands of pictures, or millions of pages of text." Id. Electronic devices like these may also be used to access cloud storage—"data located on remote servers"—as well as email and social media applications. D. 7 ¶¶ 30, 32. Data stored on electronic devices includes "personal, expressive, and associational information" like communications, location history, contact lists, internet browsing history, photos, calendars and notes. D. 7 ¶ 31. Additionally, electronic devices store "historical location information, so-called 'deleted' items that actually remain in digital storage," "metadata about digital files" and "time stamps or GPS coordinates created automatically by software on the device." D. 7 ¶ 33.

According to public CBP data, "CBP conducted 14,993 electronic device searches in the first half of fiscal year 2017," putting CBP "on track to conduct approximately 30,000 searches

this fiscal year, compared to just 8,503 searches in fiscal year 2015." D. 7 ¶ 38.[2] Searches generally come in two forms: (1) "manual" searches, during which "officers review the contents of the device by interacting with it as an ordinary user would, through its keyboard, mouse, or touchscreen interfaces"; and (2) "forensic" searches, during which officers "use sophisticated tools, such as software programs or specialized equipment, to evaluate information contained on a device," typically starting by making a copy of the device's data. D. 7 ¶¶ 39, 40, 43. Forensic searches "can capture all active files, deleted files, files in allocated and unallocated storage space, metadata . . . password-protected or encrypted data, and log-in credentials and keys for cloud accounts." D. 7 ¶ 43. On occasion, officers confiscate travelers' devices for prolonged periods. D. 7 ¶¶ 50-56.

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

A. The Search Policies

The CBP and ICE electronic device search policies detailed below are matters of public record, published by DHS and available to the public and, accordingly, may be considered by the Court for the purposes of this motion. See Alt. Energy, Inc. v. St. Paul Fire & Marine Ins. Co, 267 F.3d 30, 33 (1st Cir. 2001). Moreover, neither party challenges that the Court may take judicial

[2] See CBP Releases Statistics on Electronic Device Searches, U.S. Customs and Border Protection (Apr. 11, 2017), http://www.cbp.gov/newsroom/national-media-reliease/cbp-releases-statistics-electronic-device-searches-0. Indeed, according to CBP's reported statistics postdating Plaintiffs' amended complaint, CBP's electronic device search rate remained consistent in the second half of fiscal year 2017, which ran until September 30, 2017, and the number of travelers whose electronic devices were searched totaled 30,200. D. 18-2 at 5 n.7; CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics, U.S. Customs and Border Protection (Jan. 5, 2018), http://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive

notice of these policies, but rather, request that the Court does so. See D. 18; D. 19 at 13 n.1. The Court, therefore, takes judicial notice of the following policies: ICE's directive number 7-6.1, issued August 18, 2009, titled "Border Searches of Electronic Devices" ("ICE Policy"); CBP directive number 3340-049, issued August 20, 2009, titled "Border Searches of Electronic Devices Containing Information" ("2009 CBP Policy");[3] and CBP's directive number 3340-049A, issued January 4, 2018, superseding the 2009 CBP Policy, titled "Border Search of Electronic Devices" ("2018 CBP Policy"), D. 18-1.

1. The ICE Policy

The ICE Policy establishes procedures "to search, detain, seize, retain, and share information contained in electronic devices possessed by individuals at the border" and "applies to . . . all persons arriving in, departing from, or transitioning through the United States." ICE Pol. ¶ 1.1. It states that "[a]ll electronic devices crossing U.S. borders are subject to border search," defining "electronic devices" as "[a]ny item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices." ICE Pol. ¶¶ 8.6.1, 5.2.

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

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

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

Regarding written records of searches, "[n]othing in this policy limits the authority of Special Agents to make written notes or reports or to document impressions relating to a border encounter in ICE's paper or electronic recordkeeping systems." ICE Pol. ¶ 6.3. If ICE confiscates a device, agents must "provide the traveler with a copy of the applicable chain of custody form or other appropriate documentation." ICE Pol. ¶ 8.2.4. ICE agents may seize and retain devices or copies of information contained therein if they determine there is probable cause of unlawful activity or, to "the extent authorized by law," information "relevant to immigration, customs, and other law enforcement matters." ICE Pol. ¶¶ 8.5.1.a-b. Copies may be shared with federal, state, local and foreign law enforcement agencies. ICE Pol. ¶ 8.5.1.c.

The ICE Policy states that copies of information "determined to be of no relevance to ICE will be destroyed . . . . within seven business days after conclusion of the border search unless circumstances require additional time" and "no later than 21 calendar days after conclusion of the border search." ICE Pol. ¶ 8.5.1.e. Assisting agencies must return devices and data to ICE or

"certify to ICE that any copies in its possession have been destroyed" unless they have the independent legal authority to retain copies. ICE Pol. ¶ 8.5.2. Non-federal entities must return all copies of information "as expeditiously as possible." ICE Pol. ¶ 8.5.3.

2. The CBP Policies

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

a) The 2018 CBP Policy

The 2018 CBP Policy applies to searches performed by CBP officers, not ICE or Homeland Security Investigations ("HSI") agents. D. 18-1 ¶ 2.7. It defines "electronic device" as "[a]ny device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players." D. 18-1 ¶ 3.2.

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

All electronic device searches are documented. D. 18-1 ¶ 5.1.5. Additionally, all searches "should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, officer safety, or other operational considerations that make it inappropriate to permit the individual to remain present." D. 18-1 ¶ 5.1.6. Permission to remain present, however, "does not necessarily mean that the individual shall observe the search itself." Id.

The 2018 CBP Policy authorizes "examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications." D. 18-1 ¶ 5.1.2. The policy prohibits an officer's intentional search of information stored remotely, directing officers to request that travelers "disable connectivity to any network" prior to search. Id. According to the policy, "[t]ravelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents," and "[p]asscodes or other means of access may be requested and retained as needed to facilitate" the search. D. 18-1 ¶ 5.3.1. If an officer cannot complete an inspection because of passcode or encryption protection, the officer may "detain the device pending a determination as to its admissibility, exclusion, or other disposition" or "seek technical assistance" or "use external equipment" to access the device. D. 18-1 ¶¶ 5.3.3-4.

The 2018 CBP Policy permits officers to "detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time," which "ordinarily should not exceed five (5) days," on- or off-site, but may be extended with supervisor approval. D. 18-1 ¶ 5.4.1. If a device is detained, the officer must issue a custody receipt to the traveler prior to the traveler's departure, D. 18-1 ¶ 5.4.1.4, and all transfers of custody must be recorded, D. 18-1 ¶¶ 5.4.2.3, 5.6.2. CBP officers may make copies of electronic devices when seeking technical

assistance—e.g., device access or translation assistance—or subject matter assistance "with reasonable suspicion or national security concern." D. 18-1 ¶¶ 5.4.2.1-2. Unless assistance is sought within CBP or from ICE, requests for assistance require supervisory approval and must be documented. D. 18-1 ¶ 5.4.2.3.

If after a review of the electronic device an officer determines there is probable cause to believe it contains evidence of illegal activity, officers "may seize and retain" the device. D. 18-1 ¶ 5.5.1.1. "Without probable cause . . . CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the applicable system of records notice." D. 18-1 ¶ 5.5.1.2. The 2018 CBP Policy does not limit CBP's authority to share information from these devices, "retained in accordance with this Directive, with federal, state, local, and foreign law enforcement agencies." D. 18-1 ¶ 5.5.1.3.

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

b) The 2009 CBP Policy

Under the 2009 CBP Policy, which was in force at the time of Plaintiffs' alleged border device searches, certain policies differed. The 2009 CBP Policy did not distinguish between a basic and advanced search and no level of suspicion was required for either. D. 7 ¶ 61(a); 2009

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

B. The Plaintiffs

1. The Alasaads

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

One month later, the Alasaads' daughter's locked smartphone was searched when Nadia and her daughter arrived in New York from Morocco "where they had been visiting family." D. 7 ¶¶ 73, 75. CBP officers directed the two to a secondary inspection area. D. 7 ¶ 74. There, Nadia informed the officers that she had lost her phone, but when officers searched Nadia's purse, they

found her daughter's smartphone. Id. The officers directed the Alasaads' daughter to write down her password, and after she did, an officer "took the phone to another room for approximately 15 minutes." D. 7 ¶ 75.

2. Allababidi

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

3. Bikkannavar

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

4. Dupin

Dupin, a journalist, citizen of Haiti and legal permanent resident of the U.S. living in Massachusetts, was subject to two device searches in December 2016. D. 7 ¶¶ 17, 86-97. In the first, Dupin connected in Miami, Florida, en route from Port-au-Prince, Haiti to Montreal, Quebec, where he was visiting his daughter to take her by bus to New York City. D. 7 ¶ 86. A CBP officer escorted Dupin to a secondary inspection area in Miami, where he waited for over two hours before being escorted to a smaller room for questioning "about his work as a journalist, including the names of the organizations and specific individuals within those organizations for whom he had worked" by three CBP officers. D. 7 ¶ 87. During questioning, officers seized Dupin's locked smartphone and ordered him to provide a password, which he did. D. 7 ¶ 88. An officer searched Dupin's phone for "about two hours" during which, at certain points, the officer took Dupin's phone "into another room," returning "periodically to ask Mr. Dupin questions about the contents of the phone." D. 7 ¶ 90. The officers then returned the phone and permitted him to leave. D. 7 ¶ 91.

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

5. Gach

Gach, an artist and U.S. citizen who lives in California, had his locked smartphone searched on arrival in San Francisco from Belgium, "where he had participated in an art exhibition displaying works that could be considered critical of the government." D. 7 ¶ 18, 98-104. He was questioned "about his work as an artist and the exhibition in Belgium" in a secondary inspection area, and, when asked for his phone, told the officers that he did not want the officers to search it. D. 7 ¶ 99. After "[t]he officers told [him]that his phone would be held for an indeterminate amount of time if he did not disclose his password," Gach entered his password and handed the officers his unlocked phone. D. 7 ¶ 100. The officers searched Gach's phone "behind a dividing wall for approximately 10 minutes" and then returned the phone to him and permitted him to leave. D. 7 ¶¶ 102-04.

6. Kushkush

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

In January 2017, Kushkush flew to Washington, D.C. from Israel, where he had completed an internship with the Associated Press, carrying a "locked smartphone that he used for both professional and personal matters," the same locked laptop and unlocked devices including a digital camera, voice recorder and flash drives. D. 7 ¶ 108. In a secondary inspection area, CBP officers questioned him "about his reporting activities," asked for his social media identifiers and email address, and instructed Kushkush to unlock his phone. D. 7 ¶¶ 109-10. Kushkush

"reluctantly complied" and observed the officer manually search the phone. D. 7 ¶¶ 110-12. Officers took the other devices "into another room for approximately 20 minutes." D. 7 ¶ 112. The officers returned the devices and he was permitted to leave. D. 7 ¶ 113.

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

7. Maye

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

8. Merchant

Merchant is a U.S. citizen, founder and editor of a media organization that publishes online news content and a graduate student in international security and journalism at Harvard University. D. 7 ¶¶ 21, 125. In March 2017, after visiting her uncle in Toronto, Ontario, Merchant was directed to a secondary inspection area at a U.S. customs preclearance station in the Toronto airport prior to her flight home to Orlando. D. 7 ¶¶ 126-27. After CBP officers asked for Merchant's smartphone, Merchant—who "wears a headscarf in public in accordance with her religious beliefs"

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

9. Shibly

Shibly, a U.S. citizen and filmmaker from Buffalo, New York, had his devices searched on two occasions in January 2017. D. 7 ¶¶ 22, 136-46. First, returning home by car from Canada, Shibly was directed to a secondary inspection area at the border in New York, and told to "fill out a form with information that included . . . his phone's password." D. 7 ¶¶ 136-37. An officer then "ordered" him to provide the password, saying that "if he had nothing to hide, then he should unlock his phone," and Shibly "disengaged" the lock on the phone. D. 7 ¶¶ 137-38. Shibly also provided CBP officers with his social media identifiers. D. 7 ¶ 141. Shibly's phone was taken out of his sight for an hour before it was returned and he was permitted to leave. D. 7 ¶¶ 140, 142. Three days later, Shibly was stopped on the same bridge and directed to a secondary inspection area. D. 7 ¶¶ 143-44. When he declined to hand over his phone, "[t]hree CBP officers . . . used physical force to seize his phone." D. 7 ¶ 145. An officer took the phone—which was still unlocked from the first search—to a different room. D. 7 ¶¶ 143, 146.

10. Wright

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

IV. Procedural History

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

V. Discussion

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

A. Standing

"Standing to sue is a doctrine rooted in the traditional understanding of a case or controversy" within Article III of the U.S. Constitution, Spokeo, Inc. v. Robins, ___ U.S. ___, 136 S. Ct. 1540, 1547 (2016), and serves to "identify those disputes which are appropriately resolved through the judicial process," Whitmore v. Arkansas, 495 U.S. 149, 155 (1990). "The law of Article III standing, which is built on separation of powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches." Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013). To establish Article III standing, Plaintiffs must demonstrate that they "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." Spokeo, 136 S. Ct. at 1547; see Lujan v. Defs. of Wildlife, 504 U.S. 555, 560-61 (1992). Plaintiffs bear the burden of establishing standing, but "the same pleading standards apply both to standing determinations and Rule 12(b)(6) determinations." Hochendoner v. Genzyme Corp., 823 F.3d 724, 734 (1st Cir. 2016); see Lujan, 504 U.S. at 561; Reddy v. Foster, 845 F.3d 493, 497 (1st Cir. 2017).

"The '[f]irst and foremost' concern in standing analysis is the requirement that the plaintiff establish an injury in fact . . . ." Reddy, 845 F.3d at 500 (quoting Spokeo, 136 S. Ct. at 1547) (alteration in original). To do so, "a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" Spokeo, 136 S. Ct. at 1548 (quoting Lujan, 504 U.S. at 560). "[T]he imminence concept, while admittedly far reaching, is bounded by its Article III purpose: 'to ensure that the alleged injury is not too speculative.'" Berner v. Delahanty, 129 F.3d 20, 24 (1st Cir. 1997) (quoting Lujan, 504 U.S. at 564 n.2). Where, as here, Plaintiffs seek injunctive relief, they must plausibly allege that "the threatened injury is 'certainly impending' or there is a 'substantial

risk that the harm will occur.'" Susan B. Anthony List v. Driehaus ("SBA List"), ___ U.S. ___, 134 S. Ct. 2334, 2341 (2014) (quoting Clapper, 568 U.S. at 414, 414 n.5); see Reddy, 845 F.3d at 500. Because we are "[a]t the pleading stage, general factual allegations of injury resulting from the defendant[s'] conduct may suffice." Lujan, 504 U.S. at 561; see Hochendoner, 823 F.3d at 731.

"[S]tanding is not dispensed in gross . . . ." Lewis v. Casey, 518 U.S. 343, 358 n.6 (1996). Rather, the standing inquiry is a "plaintiff-by-plaintiff and claim-by-claim analysis." Hochendoner, 823 F.3d at 733. The Court must, therefore, determine "whether each particular plaintiff is entitled to have a federal court adjudicate each particular claim that he asserts." Id. (quoting Pagán v. Calderón, 448 F.3d 16, 26 (1st Cir. 2006)). Defendants argue that Plaintiffs do not have standing to seek declaratory or injunctive relief for any alleged Fourth or First Amendment violations and that they also lack standing to seek expungement.[4] D. 15 at 15-22. The Court addresses each claim in turn.

1. Standing to Seek Injunctive or Declaratory Relief

Plaintiffs allege that they "face a likelihood of future injury caused by the challenged policies and practices . . . related to searching and seizing electronic devices at the border." D. 7 ¶ 156. Although each Plaintiff has individual reasons for doing so, "[a]ll Plaintiffs have traveled across the U.S. border with their electronic devices multiple times" and "will continue to do so in the future." Id. At the border, "they will be subject to CBP's and ICE's policies and practices . . . namely, search or seizure of their devices absent a warrant, probable cause or reasonable

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

suspicion," and Plaintiffs cannot avoid this harm without "forego[ing] international travel or [] travel[ing] without any electronic devices, which would cause great hardship." Id. On this basis, Plaintiffs seek to enjoin Defendants from "searching electronic devices absent a warrant supported by probable cause that the devices contain" evidence of illegal activity and from "confiscating travelers' electronic devices, to effectuate searches of those devices after travelers leave the border, absent probable cause." D. 7 at 41-42.

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

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

There is no numerical threshold, however, at which likelihood of harm becomes a "substantial risk" of harm. See Kerin v. Titeflex Corp., 770 F.3d 978, 983 (1st Cir. 2014) (noting

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

Defendants also argue that Plaintiffs' allegations of future harm are impermissibly "vague" and speculative. D. 15 at 17-18. They point to Reddy for the proposition that in the First Circuit, "'[s]peculation' that a government actor 'might in the future take some other and additional action detrimental to' Plaintiffs, is 'not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm.'" D. 15 at 18 (quoting Reddy, 845 F.3d at 503). In Reddy, however, the First Circuit held that the plaintiffs' assertions of standing were speculative as to a New Hampshire buffer zone statute, emphasizing that the statute had not yet been enforced. Reddy, 845 F.3d at 496, 503. Here, by contrast, Plaintiffs challenge policies that are in place and

are being actively enforced. D. 7 ¶¶ 37-38; see SBA List, 134 S. Ct. at 2346 (finding standing to enjoin enforcement of state statute that had been enforced for decades); Dudley v. Hannaford Bros. Co., 333 F.3d 299, 306 (1st Cir. 2003) (explaining that a "real and immediate threat" of injury may be demonstrated through an "offending policy [that] remains firmly in place"). Plaintiffs' alleged future injury does not depend upon defendants' future illegal conduct untethered to a pattern of past practice, cf. Los Angeles v. Lyons, 461 U.S. 95, 102 (1983) (concluding that plaintiff subject to illegal arrest procedure made no showing that he was likely to be arrested and subjected to illegal procedure again), but rather upon recurring conduct authorized by official policies.

That is, Plaintiffs' subjection to prior searches further bolsters their allegations of likely future searches. Although "[p]ast exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief," Lujan, 504 U.S. at 564 (quoting Lyons, 461 U.S. at 102), "[p]ast wrongs [a]re evidence bearing on 'whether there is a real and immediate threat of repeated injury," Lyons, 461 U.S. at 102 (quoting O'Shea v. Littleton, 414 U.S. 488, 496 (1974)). See, e.g., Morales v. Chadbourne, 996 F. Supp. 2d 19, 37-38 (D.R.I. 2014) (finding standing for American citizen who had been inappropriately detained by ICE twice and warned that it could happen again); Thomas v. Cty. of L.A., 978 F.2d 504, 507 (9th Cir. 1992) (explaining that the "possibility of recurring injury ceases to be speculative when actual repeated incidents are documented" (quoting Nicacio v. U.S. INS, 797 F.2d 700, 702 (9th Cir. 1985))); cf. Penobscot Nation v. Mills, 861 F.3d 324, 336-37 (1st Cir. 2017) (denying standing at summary judgment where there was no evidence of prior enforcement of the policy in question against the plaintiffs). Here, all Plaintiffs have been subjected to electronics searches at the border and four Plaintiffs have been subjected to multiple device searches. D. 7 ¶¶ 2, 62-155. Plaintiffs' theory of standing, therefore, is sufficiently concrete to plausibly allege injury-in-fact.

Plaintiffs' allegations of future harm are no less concrete because they omit specific plans or dates of future travel. Defendants argue that without such details, Plaintiffs have merely expressed "some day" intentions to travel, which are not enough to establish actual or imminent injury. D. 15 at 19 (quoting Lujan, 504 U.S. at 564). In Lujan, the two individuals in question stated in affidavits that they intended to return to the habitats in question sometime "in the future," which was insufficient to establish "at the summary judgment stage, a factual showing of perceptible harm." Lujan, 504 U.S. at 563-64, 566. As a result, with plaintiffs "alleg[ing] only an injury at some indefinite future time," the Court held that the "imminence" requirement for future injury had "been stretched beyond the breaking point." Id. at 564 n.2. As Justice Kennedy explained in his concurring opinion, the requirement for travel specifics was warranted in that case because it was "not a case where it [wa]s reasonable to assume that the affiants will be using the sites on a regular basis . . . nor d[id] the affiants claim to have visited the sites since the projects commenced." Id. at 579 (Kennedy, J., concurring) (citation omitted). Plaintiffs argue that their allegations sufficiently demonstrate a "realistic risk of future exposure to [the] challenged policy," Berner, 129 F.3d at 24, through their allegations that they regularly travel outside the U.S. for work, visiting friends and family, vacation and tourism, D. 19 at 19-20; e.g., D. 7 ¶¶ 2, 62, 73, 77, 81, 86, 105, 114, 126, 143, and will continue to do so in the future, D. 7 ¶ 156.

This case is distinct from Lujan on several bases. First, this case is only at the motion to dismiss phase, unlike the summary judgment stage in Lujan, 504 U.S. at 561, 566. Second, exposure to CBP and ICE policy does not require travel to a specific destination, but rather only requires some international travel and return to the U.S.; it is reasonable to infer from the allegations in the complaint that these Plaintiffs will engage in international travel again in the future, cf. id. at 579 (Kennedy, J., concurring), particularly as Plaintiffs allege prior travel abroad

and professional backgrounds that might warrant future travel. See Lyons, 461 U.S. at 102 (looking to plaintiffs' prior actions to determine likelihood of future injury); Lujan, 504 U.S. at 592 (Blackmun, J., dissenting). Given this case's posture, the breadth of activity that would compel exposure to the policies at issue and Plaintiffs' allegations of prior travel and professional activity, Plaintiffs' allegations in this context are sufficient to allege actual or imminent injury.

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

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

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

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

2. Standing to Seek Expungement

Plaintiffs also seek expungement of all data or information "gathered from, or copies made of, the contents of Plaintiffs' electronic devices, and all of Plaintiffs' social media information and device passwords." D. 7 at 42. Retention of data illegally obtained by law enforcement may constitute continued harm sufficient to establish standing to seek expungement. See Tabbaa, 509 F.3d at 96 n.2 (stating that defendants there "properly do not contest that plaintiffs possess Article III standing based upon their demand for expungement" of data collected during border searches); Hedgepath v. Wash. Metro. Area Transit Auth., 386 F.3d 1148, 1152 (D.C. Cir. 2004) (holding plaintiff had standing to seek expungement of arrest record). Defendants challenge Plaintiffs' standing to seek expungement here. D. 15 at 20-21.

Defendants argue that, as a factual matter, standing to seek expungement has only been alleged as to one Plaintiff, Wright, whose information was allegedly extracted and not destroyed by CBP, as demonstrated through documents he obtained through a FOIA request. D. 15 at 20. Although Defendants correctly point out that "[n]either conclusory assertions nor unfounded speculation can supply the necessary heft" to establish standing, D. 15 at 20 (quoting Hochendoner, 823 F.3d at 731), Plaintiffs need not produce FOIA documentation to allege plausibly that information contained on their devices has been retained by CBP or ICE, especially given—as explained above—that this is the motion to dismiss stage of litigation.[5] Three other Plaintiffs—the Alasaads and Allababidi—also allege searches involving retention of their electronic devices for at least two weeks. D. 7 ¶¶ 70-72, 79-80. Six of the remaining seven Plaintiffs allege that during their "basic" or manual device searches, their devices were searched outside of their presence for a period of time between ten minutes and four hours.[6] D. 7 ¶¶ 84, 90, 96, 102, 107, 112, 117, 135, 140, 146. Given that both ICE and CBP policies in place at the time authorized conducting advanced searches of electronic devices without any individualized suspicion, D. 7 ¶ 58, it is plausible to infer from these facts that advanced searches may have occurred during this time, see D. 7 ¶ 84 (alleging that agents stated they used "algorithms" to search Bikkannavar's phone outside of his presence). These policies, including the 2018 CBP Policy, also sanction

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

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

creating copies of data contained on the devices during—or to be used for—advanced searches, ICE Pol. ¶ 8.1.4; D. 18-1 ¶¶ 5.1.4, 5.4.1, or to retain the assistance of other agencies and third parties, ICE Pol. ¶ 8.4.4; D. 18-1 ¶¶ 5.4.2.1-2. It is plausible, therefore, to infer that data or information from the devices may have been copied or otherwise documented during these searches.

Defendants also argue that Plaintiffs do not have standing to seek expungement because expungement would not redress Plaintiffs' alleged injury. D. 15 at 20-21. Redressability, the third standing requirement, see Spokeo, 136 S. Ct. at 1547, requires that Plaintiffs demonstrate "a likelihood that prevailing in the action will afford some redress for the injury." City of Bangor v. Citizens Commc'ns Co., 532 F.3d 70, 92 (1st Cir. 2008) (quoting Me. People's All. V. Mallinckrodt, Inc., 471 F.3d 277, 283 (1st Cir. 2006)). Plaintiffs' burden to demonstrate redressability, as with injury, is "relatively modest" at the motion to dismiss stage. Bennett v. Spear, 520 U.S. 154, 171 (1997). Plaintiffs' injury "is redressable if the relief sought can compensate the plaintiff for his losses or 'eliminate any effects' caused by a defendant's challenged conduct." Janfeshan v. U.S. Customs & Border Prot., No. 16-cv-6915, 2017 U.S. Dist. LEXIS 151058, 2017 WL 3972461, at *6 (E.D.N.Y. Aug. 21, 2017) (quoting Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 106 (1998)).

Plaintiffs have plausibly demonstrated that expungement of their data would afford some redress for their alleged injury here. Plaintiffs argue that retention of their information "compounds the violations of [their] Fourth Amendment rights, because Defendants remain free to use and exploit it or share it with other agencies that may do the same." D. 19 at 24; see Tabbaa, 509 F.3d at 96 n.2; Hedgepath, 386 F.3d at 1152. Defendants argue that expungement "would not likely result from a favorable resolution of [Plaintiffs'] claims" because "[t]he government's use

of 'evidence obtained in violation of the Fourth Amendment does not itself violate the Constitution.'" D. 15 at 20 (quoting Pa. Bd. of Prob. & Parole v. Scott, 524 U.S. 357, 362 (1998)). First, however, Defendants' argument does not go to redressability, but rather to the merits of the constitutional claim and remedy sought. Defendants do not argue that expungement would insufficiently redress Plaintiffs' alleged injury—continued violation of the Fourth Amendment through retention of Plaintiffs' data—but rather suggest that retention of Plaintiffs' data is not itself a violation of the Fourth Amendment. D. 15 at 20-21. Indeed, to the extent Plaintiffs' information was copied or obtained, subsequently retained and not destroyed by CBP or ICE, the destruction of these copies or data could redress such injury. See Janfeshan, 2017 WL 3972461, at *7.

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

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

B. Plaintiffs' Fourth Amendment Claims

The Fourth Amendment establishes that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The Fourth Amendment ensures that "the usual inferences which reasonable men draw from evidence . . . . be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime." Johnson v. United States, 333 U.S. 10, 14 (1948). "The amendment grew out of American colonial opposition to British search and seizure practices, most notably the use of writs of assistance, which gave customs officials broad latitude to search houses, shops, cellars, warehouses, and other places for smuggled goods." United States v. Wurie, 728 F.3d 1, 3 (2013), aff'd sub. nom., Riley v. California, ___ U.S. ___, 134 S. Ct. 2473 (2014).

"[T]he ultimate touchstone of the Fourth Amendment is reasonableness," Riley, 134 S. Ct. at 2482 (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)), and "reasonableness generally requires the obtaining of a judicial warrant," id. (quoting Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)). "[A] warrantless search is per se unreasonable under the Fourth Amendment, unless one of 'a few specifically established and well-delineated exceptions' applies." Wurie, 728 F.3d at 3 (quoting Arizona v. Gant, 556 U.S. 332, 338 (2009)). The border search exception, "grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country," is one such exception. United States v. Ramsey, 431 U.S. 606, 620 (1977).

Although, as an exception to the warrant requirement, border searches "have been considered to be 'reasonable' by the single fact that the person or item in question had entered into

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

By contrast, Plaintiffs argue that 'digital is different.' See D. 25 at 8.[7] They contend that the border searches at issue here run afoul of the Fourth Amendment due to the unique characteristics of electronic devices. D. 19 at 25-37. As to the border searches themselves, Plaintiffs argue that there is no meaningful distinction between basic and advanced (or manual and forensic) searches articulated in the CBP and ICE policies. D. 19 at 35. In light of the "the great volume and detail of personal information that electronic devices contain," even manual searches, they allege, are "extraordinarily invasive." D. 7 ¶ 41. See D. 7 ¶¶ 27-36. Plaintiffs allege (1) that the warrantless searches of travelers' electronic devices conducted at the border or international ports of entry, pursuant to the CBP and ICE policies, violate the Fourth Amendment, and (2) that the confiscation of devices absent probable cause violates the Fourth Amendment. D. 7 ¶¶ 169, 173. The Court begins by focusing on Plaintiffs' first Fourth Amendment claim, which

[7] An amicus brief filed by the Brennan Center for Justice, the Center for Democracy & Technology, the R Street Institute and TechFreedom details the extent to which digital devices differ from containers at issue in prior border search cases given that they "contain great quantities of extremely sensitive information." D. 25 at 7.

applies to all Plaintiffs (Count I), and then addressing Plaintiffs' confiscation claim which applies to certain of the Plaintiffs (Count III).

Six years ago, this Court was unpersuaded by the argument that, under Fourth Amendment jurisprudence, unique characteristics of cell phones and other electronic devices justified requiring a heightened level of suspicion for searches conducted at the border. House v. Napolitano, No. 11-10852-DJC, 2012 U.S. Dist. LEXIS 42297, 2012 WL 1038816, at *8 (D. Mass. Mar. 28, 2012). In House, similar to Plaintiffs here, House challenged the constitutionality of officers' search of his laptop and other electronic devices at the border under the Fourth Amendment, arguing that the search was "highly intrusive given the personal nature and quality of information stored on these devices." Id. at *6. The Court explained that in the Fourth Amendment context, "[i]t is the level of intrusiveness of the search that determines whether the search is routine, not the nature of the device or container to be searched." Id. at *8 (citing United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008)). The Court rejected House's argument, explaining that a laptop and other electronic devices are "akin to the search of a suitcase and other closed containers," which "require no particularized suspicion," id. at *7, but declined to dismiss House's Fourth Amendment claim because the prolonged detention of his electronic devices for forty-nine days was not "reasonably related in scope to the circumstances which justified it initially." Id. at *9 (quoting United States v. Cotterman, 637 F.3d 1068, 1082 (9th Cir. 2011), rev'd en banc, 709 F.3d 952 (9th Cir. 2013)).

Two years after this Court's ruling in House, as Plaintiffs point out, D. 19 at 25-31, the Supreme Court issued Riley, in which the Court held that the search-incident-to-arrest exception does not extend to cell phones, but rather the Fourth Amendment requires police to obtain a warrant supported by probable cause to search a phone seized during an arrest. Riley, 134 S. Ct. at 2494-

95. Moreover, the Supreme Court in Riley affirmed the First Circuit's ruling in Wurie, 728 F.3d at 13, which also came after this Court's ruling in House.

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

In Riley, the Supreme Court addressed the applicability of the search incident to arrest exception to cell phones and established a categorical rule requiring that officers obtain search warrants prior to searching cell phones. Riley, 134 S. Ct. at 2485. Justice Roberts, writing for a unanimous Court,[8] explained that "[a]bsent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests.'" Riley, 134 S. Ct. at 2484 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)). The Court explained that the balancing of interests did not support extending the exception "to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." Id.

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

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

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

As to the individual's privacy interests implicated, "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." Id. at 2488-89. The Supreme Court expounded at length upon the extent to which "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." Id. at 2489. Quantitatively, whereas "[m]ost people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so," cell phones have an "immense storage capacity," allowing people to carry an amount of data no longer limited by physical practicability. Id. "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions" dating back to the purchase of the phone, or earlier; "the same cannot be said of a photograph or two of loved ones tucked into a wallet." Id. Qualitatively, a person's internet browsing history, historic location information, and mobile application software (or "apps") "can form a revealing montage of the user's life." Id. at 2490. Indeed, the Court stated that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house." Id. at 2491 (emphasis in original). Moreover, the ease with which a cell phone may be used to access

remote files illustrates that a cell phone search "might extend well beyond papers and effects in the physical proximity of an arrestee," providing "yet another reason that the privacy interests here dwarf those" in prior search incident to arrest cases. Id.

The Riley court rejected the government's proposed alternative standards, including that "from the vehicle context, allowing a warrantless search of an arrestee's cell phone whenever it is reasonable to believe that the phone contains evidence of the crime of arrest." Id. at 2492. The Supreme Court explained that the exception for warrantless searches of a vehicle's passenger compartment carved out in Gant, 556 U.S. at 343, was inapplicable to cell phone searches for several reasons. Riley, 134 S. Ct. at 2492. First, the circumstances of the vehicle search involved further "reduced expectation[s] of privacy" and "heightened law enforcement needs" absent with cell phone searches. Id. (quoting Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring)); see Gant, 556 U.S. at 345. Second, crucially, the "Gant standard would prove no practical limit at all when it comes to cell phone searches," given the physical and temporal limitations present in a Gant scenario that are absent in a Riley scenario. Riley, 134 S. Ct. at 2492. The Court noted that "[i]t would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone." Id. Given the Court's "general preference to provide clear guidance to law enforcement through categorical rules," and avoid "a difficult line-drawing expedition" for officers and courts alike, the Court rejected the government's "fallback options" in favor of a warrant requirement that would apply to all cell phone searches conducted incident to arrest. Id. at 2491-93; see id. at 2497 (Alito, J., concurring) (explaining that although the Court's holding might "lead[] to anomalies," he did "not see a workable alternative" given that "[l]aw

enforcement officers need clear rules . . . and it would take many cases and many years for the courts to develop more nuanced rules").

It is also worth noting that one of the two cases on appeal in Riley was Wurie, a 2013 First Circuit opinion reversing the denial of a motion to suppress and holding that cell phones are distinct from other physical possessions that may be searched incident to arrest without a warrant. Wurie, 728 F.3d at 13-14. The First Circuit pointed to Seventh Circuit case law acknowledging that "[a]t the touch of a button a cell phone search becomes a house search, and that is not a search of a 'container' in any normal sense of that word, though a house contains data." Id. at 8-9 (quoting United States v. Flores-Lopez, 670 F.3d 803, 806 (7th Cir. 2012)). Ultimately, however, the First Circuit parted ways with the Seventh Circuit and a "majority" of jurisdictions that had upheld warrantless cell phone data searches. Id. at 5, 13. The First Circuit concluded instead that cell phone searches incident to arrest are not justified by the Chimel rationales, and that the nature and scope of the search exceeded the purposes of the warrant exception. Id. at 7-12. The court explained that cell phones store "much more personal information . . . than could ever fit in a wallet, address book, briefcase, or any of the other traditional containers that the government has invoked." Id. at 9.

Adhering to "the Supreme Court's insistence on bright-line rules in the Fourth Amendment context," the First Circuit explained that while some searches of cell phones might be less invasive than others, "it is necessary for all warrantless cell phone data searches to be governed by the same rule." Id. at 12-13. In the court's view, the government's desire for warrantless cell phone searches was "a convenient way for the police to obtain information related to a defendant's crime of arrest," and the court found no Supreme Court jurisprudence sanctioning "such a 'general evidence-gathering search.'" Id. at 13 (quoting Thornton, 541 U.S. at 632 (Scalia, J., concurring)). The

First Circuit likened the government's proposed approach to "customs officers in the early colonies [who] could use writs of assistance to rummage through homes and warehouses, without any showing of probable cause linked to a particular place or item sought," the very ill the Founders sought to eradicate with the Fourth Amendment. Id. at 9. In Riley, the Supreme Court affirmed the First Circuit's ruling. Riley, 134 S. Ct. at 2495.

2. Riley and the Border Search Exception

Defendants argue that Riley does not apply to the border search context. D. 15 at 25-27. Defendants state that "Riley itself noted that its holding was limited to the search incident to arrest context" by acknowledging that "'other case-specific exceptions may still justify a warrantless search of a particular phone.'" D. 15 at 26 (quoting Riley, 134 S. Ct. at 2492). On that basis, Defendants contend, the argument that Riley "imposes a warrant requirement" in the border search context "is without merit and has been repeatedly rejected." D. 15 at 25. Additionally, and more substantively, Defendants contend that, unlike the rationales behind the search incident to arrest exception, the border search exception "serves different and broader purposes" that "apply in full force to searches of electronic media." D. 15 at 26-27.

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

a warrant be obtained, and in this respect is like the similar 'search incident to lawful arrest' exception"). The reasoning in Riley may, therefore, carry some persuasive weight in the border search context. See, e.g., United States v. Kolsuz, 185 F. Supp. 3d 843, 856 (E.D. Va. 2016) (considering scope of privacy interest at border in light of Riley); United States v. Kim, 103 F. Supp. 3d 32, 54-58 (D.D.C. 2015) (same); cf. United States v. Camou, 773 F.3d 932, 942-43 (9th Cir. 2014) (extending Riley to the vehicle exception context); United States v. Lara, 815 F.3d 605, 610-12 (9th Cir. 2016) (applying Riley to probation search context); United States v. Henry, 827 F.3d 16, 28 (1st Cir. 2016) (rejecting defendant's Riley argument in the "plain view" context not because Riley was categorically irrelevant but because the officers had obtained a warrant prior to the smart phone search).

Additionally, the cases Defendants reference to argue that Plaintiffs' Fourth Amendment claim has been "repeatedly rejected," D. 15 at 26 n.8, carry limited weight here. The majority of these cases arose in district courts within the Ninth Circuit, where Cotterman, 709 F.3d at 968, a Ninth Circuit *en banc* decision predating Riley, still controls. See, e.g., United States v. Mendez, 240 F. Supp. 3d, 1005, 1008 (D. Ariz. 2017); United States v. Ramos, 190 F. Supp. 3d 992, 1002-03 (S.D. Cal. 2016); United States v. Lopez, No. 13-CR-2092 WQH, 2016 U.S. Dist. LEXIS 176920, 2016 WL 7370030, at *5 (S.D. Cal. Dec. 20, 2016). In Cotterman, the Ninth Circuit held that a forensic device search initiated at the border required reasonable suspicion, explaining that "the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property." Cotterman, 709 F.3d at 966. Lower courts in the Ninth Circuit are bound by the Cotterman standard, unable to apply Riley in the border context unless they find the two cases "clearly irreconcilable," which, as several courts have explained, they are not. See United States

v. Caballero, 178 F. Supp. 3d 1008, 1018 (S.D. Cal. 2016) (explaining that "[a]lthough Riley could be applied to a cell phone search at the border, this Court is bound by Cotterman"); Lopez, 2016 WL 7370030, at * 5.[9]

Here, the First Circuit has not yet spoken on what level of suspicion is required to justify a cell phone or other electronic device search at the border. The First Circuit has, however, acknowledged the significant privacy interests implicated in a cell phone search, explaining that the information on these devices is "the kind of information one would previously have stored in one's home and that would have been off-limits to officers performing a search incident to arrest." Wurie, 728 F.3d at 8. Searches of cell phones are fundamentally different from "the kinds of reasonable, self-limiting searches that do not offend the Fourth Amendment, even when conducted without a warrant." Id. at 9-10. The court also emphasized the necessity behind a bright-line rule favoring a warrant requirement, explaining that "[a] series of opinions allowing some cell phone data searches but not others, based on the nature and reasonableness of the intrusion, would create exactly the 'inherently subjective and highly fact specific' set of rules that the Court has warned against and would be extremely difficult for officers in the field to apply." Id. at 12-13 (quoting Thornton, 541 U.S. at 623).

While it is correct that neither the Supreme Court nor the First Circuit have yet held that a warrant is required for a particular type of search conducted at the border, the Court considers Plaintiffs' claim against the current legal backdrop framed by Riley and Wurie and thus turns to

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

the merits to determine whether Plaintiffs have plausibly alleged a Fourth Amendment violation for warrantless border device searches.

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

As with all Fourth Amendment exceptions, the border search exception is "subject to substantive limitations imposed by the Constitution." Ramsey, 431 U.S. at 620. The Court determines "the permissibility of a particular law enforcement practice . . . by 'balancing its intrusion on the individual's Fourth Amendment interest against its promotion of legitimate governmental interests.'" Montoya de Hernandez, 473 U.S. at 537 (quoting United States v. Villamonte-Marquez, 462 U.S. 579, 588 (1983)). "[T]he Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior." Id. at 538. Individuals have a reduced expectation of privacy at the international border, while the government's "interest in preventing the entry of unwanted persons and effects is at its zenith" there. Flores-Montano, 541 U.S. at 154, 152.

The border search slate, however, is not unlike the one on which the Supreme Court wrote in Riley. Like the border search exception's historical foundation, the search incident to arrest

exception, as the Court detailed in Riley, was "always recognized under English and American law," Riley, 134 S. Ct. at 2482 (quoting Weeks, 232 U.S. at 392). Moreover, with searches incident to arrest, the balance also tilts favorably toward the government. See id. at 2488 (explaining that "[t]he search incident to arrest exception rests not only on the heightened government interests at stake in a volatile arrest situation, but also on an arrestee's reduced privacy interests upon being taken into police custody"). The Court nevertheless explained that an arrestee's "diminished privacy interests do[] not mean that the Fourth Amendment falls out of the picture entirely." Id. Rather, the unique attributes of cell phones so increased the privacy interests of individuals that the balancing of interests that typically support the search incident to arrest exception no longer applied. See id. at 2484-85, 2488; Wurie, 728 F.3d at 9.

The border search serves the nation's "paramount interest in 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 offers "are also charged . . . with protecting this Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics, or explosives." Montoya de Hernandez, 473 U.S. at 544.

Plaintiffs argue that "warrantless searches of electronic devices are not sufficiently tethered to the narrow purposes justifying the border search exception: immigration and customs enforcement." D. 19 at 28-29. If the border exception seeks to enable officers to prevent illicit "contraband" from entering the country, see Montoya de Hernandez, 473 U.S. at 537, a search of digital data may not be necessary to achieve that aim. See Kolsuz, 185 F. Supp. 3d at 858 (explaining that digital information "is merely indirect evidence of things an individual seeks to export illegally—not the things themselves—and therefore the government's interest in obtaining this information is less significant than the government's interest in directly discovering the items to be exported illegally"); United States v. Molina-Isidoro, 267 F. Supp. 3d 900, 909 n.10 (W.D. Tex. 2016). Defendants argue that devices "can contain contraband (such as child pornography), information regarding the inadmissibility of prohibited goods or persons, or material (such as classified information, malware, or export-controlled material) that, if illicitly transferred beyond our borders, could pose a direct threat to our national security." D. 15 at 27. The Court agrees with Plaintiffs that "information regarding the inadmissibility of prohibited goods or persons," id., is distinct from contraband. D. 19 at 30 n.20; see Boyd, 116 U.S. at 623 (explaining that search and seizure of "goods liable to duties and concealed to avoid the payment thereof[] are totally different things from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him").

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

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

Additionally, although the Court agrees with Defendants that digital contraband is not "untethered" from the rationales supporting the border search exception, it is unclear at this juncture the extent to which a warrant requirement would impede customs officers' ability to ferret out such contraband.[11] "[T]he mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment." Wurie, 728 F.3d at 11 (quoting Mincey v. Arizona, 437 U.S. 385, 393 (1978)). Indeed, as Justice Roberts pointed out in Riley, "[r]ecent technological advances similar to those discussed here have, in addition, made the process of obtaining a warrant itself more efficient." Riley, 134 S. Ct. at 2493. Although a warrant might "have an impact on the ability of law enforcement to combat crime," id., it is unclear—

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

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

based on the record before the Court at this time—the extent to which such impediment justifies applying the border search exception to electronic devices. This is particularly true where the government's interests—even if they are not "untethered" to the exception's rationales—must be "[w]eighed against the significant privacy implications inherent in cell phone data searches." Wurie, 728 F.3d at 11.

On the other side of the scale, where a traveler's privacy interests are ordinarily reduced, Riley indicates that electronic devices implicate privacy interests in a fundamentally different manner than searches of typical containers or even searches of a person. Riley, 134 S. Ct. at 2488-89, 2494-95; see Wurie, 728 F.3d at 8. The Supreme Court has held that detention of a traveler at the border "beyond the scope of a routine customs search and inspection" may be justified when supported by reasonable suspicion that the traveler is smuggling contraband in their "alimentary canal," Montoya de Hernandez, 473 U.S. at 541, and that no level of suspicion is required for a border search in which officers "remove, disassemble, and reassemble a vehicle's fuel tank," Flores-Montano, 541 U.S. at 155. The First Circuit, likewise, has held that reasonable suspicion—not probable cause—is required to justify certain "nonroutine" border examinations like strip and body cavity searches. United States v. Braks, 842 F.2d 509, 512-14 (1st Cir. 1988). The First Circuit and other circuits have adopted the "routine" and "nonroutine" border search distinction first articulated in Montoya de Hernandez, 473 U.S. at 541 n.4, often distinguishing between the two by the intrusiveness of the search. See United States v. Molina-Gómez, 781 F.3d 13, 19 (1st Cir. 2015); United States v. Kelly, 302 F.3d 291, 294 (5th Cir. 2002); United States v. Ramos-Saenz, 36 F.3d 59, 61 (9th Cir. 1994).[12]

[12] The Supreme Court's dismissal of the "[c]omplex balancing tests" to determine the "degree of intrusiveness" as applied to border searches of vehicles, Flores-Montano, 541 U.S. at 152, does not eliminate the intrusiveness inquiry here. There, the Court explained that the "dignity and

Riley and Wurie indicate that electronic device searches are, categorically, more intrusive than searches of one's person or effects. See Riley, 134 S. Ct. 2489 (explaining that "[b]efore cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy"); Wurie, 728 F.3d at 8-9; United States v. Whiteside, No. 13-cr-576, 2015 U.S. Dist. LEXIS 84369, 2015 WL 3953477, at *4-5 (S.D.N.Y. June 29, 2015) (suppressing contents of digital camera searched incident to arrest based upon Riley). The ability to review travelers' cell phones allows officers to view "nearly every aspect of their lives—from the mundane to the intimate." Riley, 134 S. Ct. at 2490. Indeed, certain facts alleged here—including Nadia Alasaad's and Merchant's objections due to their photos on their phones of themselves without headscarves, D. 7 ¶¶ 67, 129—demonstrate the level of intrusiveness a manual device search can entail. The Constitutional Accountability Center, in its *amicus* brief, likens digital device searches to searches of personal papers, explaining that "personal papers increasingly take the form of digital files" kept on cell phones, laptops, and other electronic devices. D. 23 at 8. They argue personal papers require greater protection under the Fourth Amendment because these searches "'go[] to the very core of the fourth amendment right of privacy,'" given the Fourth Amendment's history and the "inherently 'personal, private nature of such papers.'" D. 23 at 18 (quoting James A. McKenna, The Constitutional Protection of Private Papers: The Role of a Hierarchical Fourth Amendment, 53 Ind. L.J. 55, 68 (1977)); see Craig M. Bradley, Constitutional Protection for Private Papers, 16 Harv. C.R.-C.L. L. Rev. 461, 483 (1981) (describing the "psychological intrusion" implicated by searches of personal papers "because the

privacy interests of the person being searched [] simply do not carry over to vehicles." Id.; see New York v. Class, 475 U.S. 106, 112-13 (1986) (explaining that vehicles implicate a diminished expectation of privacy). Under current Supreme Court jurisprudence, the opposite holds true for cell phones. See Riley, 134 S. Ct. at 2489-90.

searcher is invading not only the subject's house but his or her thoughts as well"); Ramsey, 431 U.S. at 623-24 (holding that searches for contraband in international mail did not violate the Fourth Amendment, repeatedly stressing that statutes forbade reading correspondence in the envelopes). Moreover, the potential intrusion into individuals' privacy is of "particular concern" in the border search context because the permissible scope of customs officers' investigative search is so broad and need not "be restrained by any limitations of exigency or relevance to a specific crime." Camou, 773 F.3d at 943 (explaining that the broad "allowable scope" of a search pursuant to the vehicle exception supported extending Riley's holding to cell phone searches in that context).

Defendants argue that even if device searches necessitate heightened suspicion, no higher standard could apply here than the reasonable suspicion standard.[13] D. 15 at 25; see Molina-Gómez, 781 F.3d at 19 (explaining that non-routine searches "require reasonable suspicion"). Plaintiffs argue, however, that the Supreme Court has never suggested that reasonable suspicion "is a ceiling for every border search." D. 19 at 33. Defendants emphasized at oral argument that First Circuit precedent has never required that strip searches in the border context meet a standard higher than reasonable suspicion, see Braks, 842 F.2d at 512-14, so holding digital searches to a higher standard would be incongruous. See D. 32 at 6. Notably, however, reasonable suspicion generally suffices to justify strip searches in the search incident to arrest context, too. See United States v. Barnes, 506 F.3d 58, 62 (1st Cir. 2007); Swain v. Spinney, 117 F.3d 1, 7 (1st Cir. 1997).[14]

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

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

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

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

Plaintiffs also argue that even if Riley does not apply here, "border search precedent provides a parallel justification for requiring a warrant based on probable cause for border searches of electronic devices." D. 19 at 31. Given that the Court has concluded that Riley has some weight

---

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

in the border search context and that, on that basis, Plaintiffs have stated a plausible Fourth Amendment claim, the Court need not reach this further argument.

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

3. Plaintiffs' Confiscation Claim

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

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

detention of a locked laptop, flash drive and camera raised a plausible Fourth Amendment claim, despite dismissing claim regarding the search itself); Cotterman, 709 F.3d at 966-67.

Plaintiffs argue that confiscations pursuant to CBP and ICE policies are "excessive" in scope and duration. D. 7 ¶¶ 56(b)-(c). As this Court has previously explained, "the inquiry into the reasonableness of the duration of a seizure is . . . an appropriate consideration under the Fourth Amendment analysis" even at the border. House, 2012 WL 1038816, at *9 (citing Place, 462 U.S. at 709-10); see United States v. Mitchell, 565 F.3d 1347, 1351-52 (11th Cir. 2009) (holding that a twenty-one day delay in securing a warrant for a laptop search was unreasonable). Defendants argue that Plaintiffs' claim is baseless given that the official policies limit detentions to "a brief, reasonable period of time." D. 15 at 34 (quoting D. 18-1 ¶ 5.3.1). The lengths of the detentions alleged here, however—including ten months for Allababidi and fifty-six days for Wright—suggest that the Fourth Amendment may require clearer guidance than that. See Riley, 134 S. Ct. at 2492-93 (reiterating the necessity of "clear guidance" in the Fourth Amendment context).

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

C. Plaintiffs' First Amendment Claim

Finally, Defendants seek dismissal of Plaintiffs' claim, Count II, that they "violate the First Amendment by searching electronic devices that contain expressive content and associational information, absent a warrant supported by probable cause," D. 7 ¶ 171. D. 14 at 2. The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble." U.S. Const. amend. I. These rights "are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference." Bates v. City of Little Rock, 361 U.S. 516, 523 (1960). As the Supreme Court has explained, "associational rights . . . can be abridged even by government

actions that do not directly restrict individuals' ability to associate freely." Lyng v. Int'l Union, UAW, 485 U.S. 360, 367 n.5 (1988); see AFL-CIO v. FEC, 333 F.3d 168, 175 (D.C. Cir. 2003) (explaining that compulsory "disclosure of political affiliations and activities can impose just as substantial a burden on First Amendment rights as can direct regulation"); Baird v. State Bar of Ariz., 401 U.S. 1, 6-7 (1971) (explaining that "[w]hen a State seeks to inquire about an individual's beliefs and associations a heavy burden lies upon it to show that the inquiry is necessary to protect a legitimate state interest").

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

Plaintiffs argue that to justify digital device searches, "[t]he government must have a compelling interest in the information and use narrowly tailored means that do not seek more information than necessary." D. 19 at 38. The Court is not convinced that such strict scrutiny

applies here, where CBP and ICE policies are content-neutral, see Asociacion de Educacion Privada de P.R., Inc. v. Garcia-Padilla, 490 F.3d 1, 15-16 (1st Cir. 2007), and, although potentially burdening speech, do not prevent anyone from speaking, Sindicato Puertotorriqueño de Trabajadores v. Fortuño, 699 F.3d 1, 12 (1st Cir. 2012). In general, however, compelled disclosure of First Amendment protected activity "cannot be justified by a mere showing of some legitimate governmental interest." Buckley v. Valeo, 424 U.S. 1, 64 (1976). Rather, "even if any deterrent effect on the exercise of First Amendment rights arises, not through direct government action, but indirectly as an unintended but inevitable result of the government's conduct in requiring disclosure," there must be a "'substantial relation between the governmental interest and the information required to be disclosed." Id. at 64-65; see Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539, 546 (1963). The Court must, therefore, determine whether the complaint adequately alleges an interference with First Amendment rights that is "direct and substantial" or "significant." House, 2012 WL 1038816, at *12 (quoting Fighting Finest v. Bratton, 95 F.3d 224, 228 (2d Cir. 1996)). Plaintiffs argue that given the technological capacities of electronic devices, the government's broad search policies "impose[] a substantial burden on First Amendment rights without justification." D. 19 at 41.

Defendants do not argue that warrantless searches would not be a significant or substantial burden on travelers' First Amendment rights, nor do they explain their assertion that a heightened standard is not "required by the First Amendment." D. 32 at 6 n.4. Rather, Defendants argue that "the border search doctrine is not subject to a First Amendment exception," and that if it were, the consequences would be "staggering." D. 15 at 29 (quoting Ickes, 393 F.3d at 507, 506). As a general matter, "[t]hat the initial search and seizure occurred at the border does not strip [Plaintiffs] of [their] First Amendment rights." House, 2012 WL 1038816, at *13; Tabbaa, 509 F.3d at 102

n.4 (explaining that a routine search may constitute a "significant or substantial burden on plaintiffs' First Amendment associational rights").

Moreover, the Court is not persuaded that Ickes, 393 F.3d at 506, upon which Defendants rely, provides appropriate guidance here. This Court need not carve out an exception for all expressive material to find a plausible claim has been stated that digital device searches unjustifiably burden travelers' First Amendment rights. See House, 2012 WL 1038816, at *13 (holding that the plaintiff stated plausible First Amendment claim for his cell phone search despite failing to state plausible Fourth Amendment claim). The Supreme Court's distinction between cell phones and other expressive materials in Riley, postdating the Fourth Circuit's ruling in Ickes, further illustrates this point. See Riley, 135 S. Ct. at 2490. Additionally, in Ickes, the Fourth Circuit was concerned with the "headaches" such a First Amendment "exception" would bring for customs officers. Ickes, 393 F.3d at 506. What Plaintiffs seek as a remedy here, however, is "simple—get a warrant," Riley, 134 S. Ct. at 2495. D. 19 at 39. Finally, in Ickes, the Fourth Circuit assured that the defendant's warning that "any person carrying a laptop computer . . . on an international flight would be subject to a search of the files on the computer hard drive" was "far-fetched," Ickes, 393 F.3d at 506-07. Plaintiffs point to the recent increase in border device searches and the expanding storage and functioning capacities of electronic devices to suggest otherwise. D. 7 ¶¶ 30, 38; D. 19 at 41.

Defendants also argue that this Court's reasoning in House does not apply here. D. 15 at 29. They contend that "the facts of that case are easily distinguished," where, unlike here, House alleged he was targeted for investigation because of his specific expressive or associational activities. Id.; see House 2012 WL 1038816, at *10-11. First, certain Plaintiffs allege facts prior to their device searches that are not dissimilar to those in House: while Dupin's phone was being

searched, he was questioned "about his work as a journalist, including the names of the organizations and specific individuals within those organizations for whom he had worked"; Gach was questioned "about his work as an artist" prior to searching his phone; Kushkush was asked about "his reporting activities"; and Merchant was questioned at secondary inspection about her "religious affiliation" and her blog. D. 7 ¶¶ 87, 93, 99, 109, 133. One *amicus* argues that journalists "are particularly vulnerable to targeted surveillance by means of suspicionless device searches." D. 26 at 13. As in House, such allegations are "pertinent" to Plaintiffs' First Amendment claim because they suggest that the officers' "motivation to search and retain [Plaintiffs'] devices" was to examine expressive or associational material. House, 2012 WL 1038816, at *10.

Second, the reasoning in House was not limited to targeting allegations alone. The Court explained there that the seizure of House's laptop and other devices gave the government possession of confidential lists of organizational members and supporters, as well as emails and documents detailing House's organization's inner workings. House, 2012 WL 1038816, at *12. Such "[c]ompulsory disclosure . . . 'can seriously infringe on privacy of association and belief guaranteed by the first amendment,' and can 'have . . . a profound chilling effect.'" Id. (quoting Buckley, 424 U.S. at 64; Perry v. Schwarzenegger, 591 F.3d 1126, 1135 (9th Cir. 2009)) (internal citations omitted). Here, the CBP and ICE policies broadly permit suspicionless searches in pursuit of "information," ICE Pol. ¶¶ 5.2, 6.1; D. 18-2 ¶ 5.1.3, which could reasonably include such searches within their ambit. In Ramsey, as Plaintiffs point out, D. 19 at 40, the Supreme Court held that the statutory scheme permitting warrantless search of incoming international mail did not violate the constitution because it applied only when there was reason to believe the envelopes contained physical items and regulations "flatly prohibit[ed], under all circumstances,"

customs officials from reading correspondence without a warrant. Ramsey, 431 U.S. at 623. The Court did not "decide whether, in the absence of the regulatory restrictions, speech would be 'chilled,' or, if it were, whether the appropriate response would be to apply the full panoply of Fourth Amendment requirements." Id. at 624 n.18. Here, there are no similar First Amendment safeguards in the CBP and ICE electronic device policies.

In light of the particular concerns raised by digital devices like cell phones detailed above, see Riley, 134 S. Ct. at 2489-91, and the limitless search authorizations in the CBP and ICE policies, Plaintiffs have plausibly alleged that the government's digital device search policies substantially burden travelers' First Amendment rights.[15]

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

VI. Conclusion

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

So Ordered.

/s/ Denise J. Casper
United States District Judge

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