United States Court of Appeals
For the First Circuit

Nos. 20-1077
20-1081

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

Plaintiffs, Appellees/Cross-Appellants,

v.

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

Defendants, Appellants/Cross-Appellees.

---

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

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

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

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

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

Before

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

Joshua Paul Waldman, Appellate Staff, Civil Division U.S. Department of Justice, with whom Joseph H. Hunt, Assistant Attorney General, Scott R. McIntosh, Appellate Staff, Civil Division U.S. Department of Justice, and Andrew E. Lelling, United States Attorney, were on briefs, for appellants/cross-appellees.

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

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

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

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

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

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

Elizabeth B. Wydra, Brianne J. Gorod, Brian R. Frazelle, and

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

Dayna J. Zolle on brief for Constitutional Accountability Center, amicus curiae.

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

February 9, 2021

LYNCH, Circuit Judge. Plaintiffs bring a civil action seeking to enjoin current policies which govern searches of electronic devices at this country's borders. They argue that these border search policies violate the Fourth and First Amendments both facially and as applied. The policies each allow border agents to perform "basic" searches of electronic devices without reasonable suspicion and "advanced" searches only with reasonable suspicion. In these cross-appeals we conclude that the challenged border search policies, both on their face and as applied to the two plaintiffs who were subject to these policies, are within permissible constitutional grounds. We find no violations of either the Fourth Amendment or the First Amendment. While this court apparently is the first circuit court to address these questions in a civil action, several of our sister circuits have addressed similar questions in criminal proceedings prosecuted by the United States. We join the Eleventh Circuit in holding that advanced searches of electronic devices at the border do not require a warrant or probable cause. United States v. Vergara, 884 F.3d 1309, 1311-12 (11th Cir. 2018). We also join the Ninth and Eleventh Circuits in holding that basic border searches of electronic devices are routine searches that may be performed without reasonable suspicion. United States v. Cano, 934 F.3d 1002, 1016 (9th Cir. 2019), petition for cert. filed (Jan. 29, 2021) (No. 20-1043); United States v. Touset, 890 F.3d 1227,

1233 (11th Cir. 2018). We also hold the district court erroneously narrowed the scope of permissible searches of such equipment at the border.[1]

I. Facts

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

A. Agency Policies

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

The first policy is CBP Directive No. 3340-049A, Border Search of Electronic Devices (2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf (the "CBP Policy"). The CBP Policy "provide[s] guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in . . . mobile phones . . . and any other communication, electronic, or digital devices . . . to ensure compliance with customs, immigration, and other laws that CBP is

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

authorized to enforce and administer." CBP Policy at 1.[2] The CBP Policy defines an "electronic device" as "[a]ny device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players." Id. at 2. The CBP Policy does not address CBP's authority to search electronic devices with a warrant, consent, or in response to exigent circumstances. Id.

The CBP Policy distinguishes between "basic" and "advanced" searches.[3] It defines an "advanced search" as "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." Id. at 5. Advanced searches require "supervisory approval" and under the CBP Policy may only be performed "[i]n instances in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern." Id. A "basic search" is any non-advanced search. Id. at 4. The CBP Policy states that a basic search may be performed "with or without suspicion." Id.

---

[2] The policy is mandatory. CBP Policy at 1 ("All CBP Officers . . . shall adhere to the policy." (emphasis added)).

[3] "Advanced" searches are sometimes referred to as "forensic" searches. Though the terms are not precisely co-extensive, any difference is immaterial here.

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

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

The second policy is Immigration and Customs Enforcement Directive No. 7-6.1, Border Searches of Electronic Devices (2009), https://hdhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf, ("ICE Directive") as superseded in part by Immigration and Customs Enforcement Broadcast: Legal Update -- Border Search of Electronic Devices (2018) ("ICE Broadcast"), (together "ICE Policy" and, together with the CBP Policy, the "Policies"). The ICE Policy governs ICE's searches of electronic devices at the border "to ensure compliance with customs, immigration, and other laws enforced by ICE." ICE Directive at 1. The policy defines an "electronic device" as "any item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices." ICE Directive at 2. The policy allows for suspicionless basic searches but states that as of May 11, 2018, ICE agents "should no longer perform advanced border searches of electronic devices without

reasonable suspicion." ICE Broadcast. The ICE Policy also allows agents to detain electronic devices for a "reasonable time given the facts and circumstances of the particular search." ICE Directive at 4.

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

B. The Searches of Plaintiffs' Electronic Devices

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

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

II. Procedural History

Plaintiffs filed suit on September 13, 2017 -- before the effective date of the challenged Policies -- alleging that CBP and ICE violated the Fourth and First Amendments by performing various types of searches of electronic devices without warrants and violated the Fourth Amendment by retaining plaintiffs'

electronic devices for an extended period absent probable cause.[4] The plaintiffs sought declaratory and injunctive relief, including expungement of "all information gathered from, or copies made of, the contents of Plaintiffs' electronic devices."

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

After discovery, the parties filed cross-motions for summary judgment. The district court granted in part and denied in part plaintiffs' motion for summary judgment and denied the government's motion for summary judgment. Alasaad, 419 F. Supp. 3d at 174. The district court also held that plaintiffs had standing to seek declaratory and injunctive relief as well as expungement of their data from CBP and ICE databases. Id. at 151-54.[5]

As to the merits of the Fourth Amendment challenges, the district court first held that basic and advanced searches are

---

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

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

[5] The government does not challenge plaintiffs' standing on appeal.

both "non-routine" searches, and thus that both types of searches required reasonable suspicion.[6] Id. at 163, 165. The court concluded that the basic search component of the Policies violated the Fourth Amendment. Id. at 165, 168.

As to the scope of both basic and advanced searches permitted under the Policies, the court found two constitutional violations. It reasoned that because the border search exception is premised on the government's paramount interest in "stopping contraband at the border," "the reasonable suspicion that is required . . . is . . . that the electronic devices contain[] contraband [itself]," rather than (a) evidence of contraband or (b) evidence or information regarding other crimes enforced at the border. Id. at 166. Thus, the Policies were unconstitutional because they did not restrict agents to searches for contraband contained in the devices themselves and allowed border searches as to evidence of all crimes CBP or ICE are authorized to enforce.[7] CBP Policy at 1, 5; ICE Directive at 1, 2.

---

[6] The district court noted that a "cursory search of an electronic device -- e.g., a brief look reserved to determining whether a device is owned by the person carrying it across the border, confirming that it is operational and that it contains data . . . [would] not require a heightened showing of cause." Alasaad, 419 F. Supp. 3d at 163.

[7] ICE and CBP are authorized to enforce a broad spectrum of laws. See, e.g., 6 U.S.C. § 211(c)(5) (requiring CBP to "detect, respond to, and interdict terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States"); id. § 211(c)(11) (requiring CBP to "enforce and administer the laws

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

The district court granted declaratory relief stating that

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

Id. at 173.

The district court declined to grant broad injunctive relief based on its finding of constitutional violations. Id. at 174. It did enjoin the government from searching or detaining any of plaintiffs' electronic devices at the border absent "reasonable suspicion that the device contains contraband," and from detaining

---

relating to agricultural import"); 31 U.S.C. §§ 5316-17 (authorizing warrantless border searches to enforce limitations on transferring $10,000 or more out of the United States); 19 C.F.R. § 12.39 (authorizing CBP to enforce law restricting the importation of "articles involving unfair methods of competition").

plaintiffs' electronic devices for "longer than a reasonable period."

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

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

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

III. Analysis

We review a grant of summary judgment de novo. Henderson v. Mass. Bay Transp. Auth., 977 F.3d 20, 29 (1st Cir. 2020). "Cross-motions for summary judgement do not alter the basic . . . standard, but rather simply require us to determine whether either of the parties deserves judgment as a matter of law on facts that are not disputed." Adria Int'l. Grp., Inc. v. Ferre Dev., Inc., 241 F.3d 103, 107 (1st Cir. 2001).

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

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

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

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

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

> [a]bsent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."

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

One such exception to the warrant requirement, recognized from early in our history, is the border search exception. See Boyd v. United States, 116 U.S. 616, 623 (1886); Carroll v. United States, 267 U.S. 132, 153-54 (1925). The exception is grounded in the government's "inherent authority to

protect, and a paramount interest in protecting, its territorial integrity." United States v. Flores-Montano, 541 U.S. 149, 153 (2004). Further, "the expectation of privacy [is] less at the border than in the interior . . . [and] the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border." United States v. Montoya de Hernandez, 473 U.S. 531, 539-40 (1985).

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

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

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

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

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

Further, given the volume of travelers passing through our nation's borders, warrantless electronic device searches are essential to the border search exception's purpose of ensuring that the executive branch can adequately protect the border. See

Montoya de Hernandez, 473 U.S. at 544 (stating that border officials are "charged . . . with protecting this Nation from entrants who may bring anything harmful into this country"). A warrant requirement -- and the delays it would incur -- would hamstring the agencies' efforts to prevent border-related crime and protect this country from national security threats.

Every circuit that has faced this question has agreed that Riley does not mandate a warrant requirement for border searches of electronic devices, whether basic or advanced. The Eleventh Circuit held that "[b]order searches have long been excepted from warrant and probable cause requirements, and the holding of Riley does not change this rule." Vergara, 884 F.3d at 1312-13. The Fourth Circuit held after Riley that "law enforcement officers may conduct a warrantless forensic search of a cell phone under the border search exception where the officers possess sufficient individualized suspicion of transnational criminal activity." United States v. Aigbekaen, 943 F.3d 713, 719 n.4 (4th Cir. 2019).[9] The Ninth Circuit, noting that even "post-Riley, no court has required more than reasonable suspicion to justify even an intrusive border search," held that both basic and advanced

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

border searches may be performed without a warrant or probable cause. Cano, 934 F.3d at 1015-16.

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

2. Basic Searches May Be Performed Without Reasonable Suspicion

Agents may perform "routine" searches at the border without reasonable suspicion. Montoya de Hernandez, 473 U.S. at 538, 541. Under this circuit's law, certain "non-routine" searches must be grounded on reasonable suspicion. United States v. Molina-Gómez, 781 F.3d 13, 19 (1st Cir. 2015); United States v. Braks, 842 F.2d 509, 513-14 (1st Cir. 1988). Whether a border search is routine or non-routine depends on an assessment of the facts of the case. Braks, 842 F.2d at 512 (holding that request to female at border to lift skirt was routine search); Molina-Gómez, 781 F.3d at 19 (holding that the search of a laptop and PlayStation, whether routine or non-routine, was justified because reasonable suspicion existed); United States v. Robles, 45 F.3d 1, 5 (1st Cir. 1995) (holding, where the government conceded that drilling into metal cylinder was non-routine search, that the search was justified by reasonable suspicion). Subjecting individuals to strip searches or body-cavity searches are examples of non-routine searches. Molina-Gómez, 781 F.3d at 19.

Plaintiffs argue that because electronic devices may contain a trove of sensitive personal information, basic border

searches of electronic devices are non-routine searches requiring at least reasonable suspicion. While, as noted above, Riley's warrant requirement in the search incident to arrest context does not extend to border searches, Riley recognized that modern electronic devices "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse" and "differ in both a quantitative and qualitative sense from other objects that might be kept on [a traveler's] person." 573 U.S. at 393. These privacy concerns, however significant or novel, are nevertheless tempered by the fact that the searches are taking place at the border, where the "Government's interest in preventing the entry of unwanted persons and effects is at its zenith," Flores-Montano, 541 U.S. at 152, and the "Fourth Amendment balance of interests leans heavily to the Government," Montoya de Hernandez, 473 U.S. at 544. Electronic device searches do not fit neatly into other categories of property searches, but the bottom line is that basic border searches of electronic devices do not involve an intrusive search of a person, like the search the Supreme Court held to be non-routine in Montoya de Hernandez. 473 U.S. at 541 & n.4. Basic border searches also require an officer to manually traverse the contents of the traveler's electronic device, limiting in practice the quantity of information available during a basic search. The CBP Policy only allows searches of data resident on the device. CBP Policy at 4. And a basic border

search does not allow government officials to view deleted or encrypted files.[10]

We thus agree with the holdings of the Ninth and Eleventh circuits that basic border searches are routine searches and need not be supported by reasonable suspicion. Cano, 934 F.3d at 1016; Touset, 890 F.3d at 1233; see also United States v. Kolsuz, 890 F.3d 133, 146 n.5 (4th Cir. 2018) (stating that United States v. Ickes, 393 F.3d 501 (4th Cir. 2005) "treated a [basic] search of a computer as a routine border search, requiring no individualized suspicion for the search").

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

Plaintiffs next argue that border searches of electronic devices "must be limited to searches for contraband." This argument is premised on plaintiffs' assertions that the border search exception (a) extends only to searches aimed at preventing the importation of contraband or entry of inadmissible persons and (b) covers only searches for contraband itself, rather than

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

for evidence of border-related crimes or contraband. The argument fails and its premises are incorrect.

In non-border contexts the Supreme Court has held that warrantless searches "must be limited in scope to that which is justified by the particular purposes served by the exception." Florida v. Royer, 460 U.S. 491, 500 (1983) (plurality opinion); see also Riley, 573 U.S. at 386. Riley did not purport to extend this rule to the border search context. Even assuming arguendo that the analysis used in Riley applies here, such an analysis would only require that warrantless border searches be tethered to "the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country."[11] Flores-Montano, 541 U.S. at 152 (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977)). Further, the Supreme Court has repeatedly said that routine searches "are reasonable simply by virtue of the fact that they occur at the border." Id. at 152-53 (quoting Ramsey, 431 U.S. at 616). This is so because the government's interest in preventing crime at international borders "is at its zenith," see id., and it follows that a search for evidence of either contraband or a cross-border crime furthers the purposes of the border search exception to the warrant requirement.

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

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

Congress is better situated than the judiciary to identify the harms that threaten us at the border.[12] Kolsuz, 890 F.3d at 152 (Wilkinson, J, concurring in the judgment) ("[Riley does not] begin to answer the question of who should strike the balance between privacy and security at the border of the

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

country."); see also Riley, 573 U.S. at 408 (Alito, J., concurring in part and concurring in the judgment) (stating with respect to the reasonableness of warrantless searches of mobile phones that "[l]egislatures . . . are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future"). In weighing the competing policy considerations, Congress or the Executive may choose to strike a different balance as to border searches of electronic devices and may choose to grant greater protection than required by the Constitution.

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

contraband and documentary evidence of a crime is without legal basis").[13]

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

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

C. Device Detention

Plaintiffs further argue that the CBP and ICE Policies violate the Fourth Amendment because they do not impose an "effective limit on [the] duration" of electronic device detentions.[14] Plaintiffs' argument is in the abstract as they have not presented any facts concerning the actual retention of devices pursuant to the policies at issue.

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

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

The nature of plaintiffs' challenge is unclear. The Policies permit detention for only a reasonable period, which is the constitutional test. See Montoya de Hernandez, 473 U.S. at 544. If the argument is that "reasonable" must be replaced with hard time limits, the Supreme Court has rejected that proposition. Id. at 543. If the argument is that the judgment as to reasonableness should not be left in the first instance to the agent who conducts the search, that misreads the Policies. The CBP Policy requires a supervisor's permission to detain a device after its owner leaves the border, a higher level of supervisory approval to extend a detention for longer than five days, and a third level of approval to extend a detention beyond fifteen days. CBP Policy at 7. What is reasonable is surely fact specific and future as applied attacks are not foreclosed should there be abuses.[15]

D. First Amendment

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

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

impermissibly chill speech.[16] They further argue that such searches unduly interfere with the First Amendment freedoms to "'engage in association' . . . without government scrutiny, . . . speak anonymously, . . . receive unpopular ideas, confidentially and without government scrutiny, . . . read books and watch movies privately . . . [and] gather and publish newsworthy information absent government scrutiny."

Because plaintiffs seek relief "beyond [their] particular circumstances," "they must 'satisfy [the] standards for a facial challenge to the extent of that reach.'" Proj. Veritas Action Fund v. Rollins, 982 F.3d 813, 826 (1st Cir. 2020) (emphasis omitted) (quoting John Doe No. 1 v. Reed, 561 U.S. 186, 194 (2010)). Thus, plaintiffs must show that "a substantial number of [the ICE and CBP Policies'] applications are unconstitutional,

---

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

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

judged in relation to the statute's plainly legitimate sweep." United States v. Stevens, 559 U.S. 460, 473 (2010) (quoting Wash. State Grange v. Wash. State Republican Party, 552 U.S. 442, 449 n.6 (2008)).

The First Amendment provides protections -- independent of the Fourth Amendment -- against the compelled disclosure of expressive information. See Buckley v. Valeo, 424 U.S. 1, 64 (1976); Tabbaa v. Chertoff, 509 F.3d 89, 102 n.4 (2d Cir. 2007) (analyzing First Amendment challenge to targeted border searches independently of Fourth Amendment); Ramsey, 431 U.S. at 623-24. Neither this circuit nor the Supreme Court has specified the appropriate standard to assess alleged government intrusions on First Amendment rights at the border. See Ramsey, 431 U.S. at 623-24 (refusing to "consider the constitutional reach of the First Amendment in this area"); see also Tabbaa, 509 F.3d at 102 n.5 ("It may also be true that the First Amendment's balance of interests is qualitatively different where, as here, the action being challenged is the government's attempt to exercise its broad authority to control who and what enters the country.").

Under any standard plaintiffs have not shown that the content-neutral border search Policies facially violate the First Amendment. See Ramsey, 431 U.S. at 623 ("More fundamentally, however, the existing system of border searches has not been shown to invade protected First Amendment rights, and hence there is no

reason to think that the potential presence of correspondence makes the otherwise constitutionally reasonable search 'unreasonable.'" (footnote omitted)). The Policies have a plainly legitimate sweep and serve the government's paramount interests in protecting the border.[17]

Nor, as plaintiffs contend, does the presence of expressive material on electronic devices "trigger[] a warrant requirement." A higher level of suspicion is not generally required to search potentially expressive materials. See New York v. P.J. Video, Inc., 475 U.S. 868, 875 (1986); United States v. Brunette, 256 F.3d 14, 16 (1st Cir. 2001) (holding the probable cause standard "is no different where First Amendment concerns may be at issue"); see also Ickes, 393 F.3d at 507 (refusing to apply a different standard to border searches of expressive material); United States v. Arnold, 533 F.3d 1003, 1010 (9th Cir. 2008) (same).

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

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

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

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

E. Expungement

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

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

IV. Conclusion

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