Nos. 20-1077, 20-1081

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

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

Plaintiffs-Appellees/Cross-Appellants,

v.

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

Defendants-Appellants/Cross-Appellees.

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

APPELLANTS' REPLY BRIEF AND CROSS-APPELLEE ANSWERING BRIEF

JEFFREY BOSSERT CLARK
Acting Assistant Attorney General

ANDREW E. LELLING
United States Attorney

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

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES (CONT'D)

Page(s)

Cases

TABLE OF AUTHORITIES (CONT'D)

Page(s)

Cases

TABLE OF AUTHORITIES (CONT'D)

Page(s)

Cases

TABLE OF AUTHORITIES (CONT'D)

Page(s)

Cases

Statutes

TABLE OF AUTHORITIES (CONT'D)

Page(s)

Statutes

Regulations

INTRODUCTION

1. The CBP and ICE Directives do not violate the Fourth Amendment. No court, either before or after *Riley v. California*, 573 U.S. 373 (2014), has accepted plaintiffs' argument that a border search of an electronic device requires probable cause and a warrant. *Riley* addressed a search incident to arrest in the domestic interior, whereas a border search entails entirely different considerations. In the border context, a person's expectations of privacy are lower, the Government's interest in preventing the entry of unwanted persons and goods is at its zenith, and the Fourth Amendment balancing of interests is therefore struck much more favorably for the Government. Plaintiffs' argument would mean, quite implausibly, that the search of an electronic device at the border requires *more* suspicion (probable cause and warrant) than the highly-intrusive, intimate exposure involved in border strip-searches or body-cavity searches (reasonable suspicion).

The agencies' Directives also comply with any applicable Fourth Amendment requirement for reasonable suspicion. Three courts of appeals agree that no suspicion is required for a basic search of an electronic device, and no circuit has reached a contrary conclusion. While two appellate courts require heightened suspicion for a forensic search, the Directives meet any such requirement because they already require reasonable suspicion for an advanced search in which officers connect external equipment to review, copy and/or analyze the contents of an electronic device. Plaintiffs' argument that a heightened suspicion requirement should be

applied to a basic search lacks merit and defies common sense. Both the Fourth and Ninth Circuit distinguished between a basic search in which officers manually examine pictures, texts, or phone records, and a search using powerful forensic tools to copy and catalog hundreds of gigabytes of information, producing a comprehensive analysis of data stored on the device, including deleted data that cannot otherwise be viewed. The Fourth Amendment analysis frequently takes into account the use of significant advancements in technology that reveal to the Government information beyond what could otherwise be observed by conventional methods as, for example, with thermal-imaging devices, GPS monitors, and cell-site location information.

2. Plaintiffs also err in contending that a border search of an electronic device is limited to the search for digital contraband itself, and does not permit a search for evidence of contraband smuggling or other border-related offenses. That distinction makes no sense in terms of the purposes of the border search exception. A search for evidence of contraband and a search for contraband itself equally serve the Government's interest in interdicting contraband before it enters the country, or in enforcing other applicable provisions regulating who or what may cross the border. Plaintiffs erroneously rely on *Boyd v. United States*, 116 U.S. 616, 623 (1886), which drew a distinction between a search for contraband and a search for evidence. The Supreme Court, however, long ago overruled *Boyd*'s distinction in unambiguous and sweeping terms because it lacked any grounding in the text of the Fourth Amendment, bore no logical relationship to personal expectations of privacy, imposed

an unworkable distinction between contraband and evidence, and was predicated on the discredited view that Fourth Amendment rights are controlled by property interests alone.

3. The agencies' Directives specify that an electronic device may only be detained for a "reasonable" period of time to conduct a border search, and the district court correctly declined to impose a more precise time limit given the Supreme Court's consistent rejection of hard-and-fast limits on the duration of a Fourth Amendment seizure, particularly at the border. Plaintiffs agree that the duration must be "reasonable," but do not explain how this Court could adopt a more concrete limitation without imposing the very kind of rigid rule the Supreme Court rejects. And plaintiffs' suggestion that a 12-day seizure of one plaintiff's device is necessarily unreasonable cannot be squared with this Court's holding that CBP did not act unreasonably in detaining a device for 22 days. *United States v. Molina-Gomez*, 781 F.3d 13, 21 (1st Cir. 2015).

4. Plaintiffs erroneously argue that the First Amendment requires a heightened standard for a border search of an electronic device containing expressive material. Plaintiffs' argument is difficult to square with the Supreme Court's rejection of a higher Fourth Amendment standard for a warrant to search materials protected by the First Amendment. Both the Fourth and Ninth Circuit have reached the same conclusion with respect to a border search of an electronic device, correctly reasoning that imposing a higher Fourth Amendment standard as plaintiffs suggest would create

an unjustified exception undermining the very purpose of the border search doctrine, and would impose an unwise and unworkable requirement for border officers to make snap decisions about what materials are deemed expressive under the First Amendment.

5. Finally, the district court did not abuse its discretion in declining to issue the equitable remedy of expungement. A court's authority to do so is narrow, and the district court permissibly reasoned that the Government's compelling interest in protecting the border, combined with the good-faith actions of officers operating in an uncertain and rapidly-evolving area of the law, counseled against the grant of such relief. Moreover, expungement is not warranted because there is no Fourth Amendment violation in this case. Virtually all plaintiffs allege nothing more than a basic search, and every appellate court has agreed such a search requires no suspicion at all. Only a single plaintiff alleges both an advanced search and the retention of records that could be expunged, but that advanced search occurred under CBP's old policy that has been superseded by the current Directive requiring reasonable suspicion. Expungement is not warranted for a single plaintiff in those circumstances. Granting relief would require this Court to unnecessarily resolve the antecedent question of whether the now-defunct Directives comply with the Fourth Amendment where otherwise that constitutional question could otherwise be avoided, and granting expungement of record retained by the an agency actions pursuant to a now-

superseded policy could have no possible deterrent effect on the agency's conduct going forward under its current Directives.

ARGUMENT

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

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

Plaintiffs contend that any search of an electronic device at the border requires probable cause and a warrant, Pls. Br. 17-23, arguing that *Riley v. California*, 573 U.S. 373 (2014) – which held that the search of data on a cell phone seized during an arrest requires a warrant and probable cause – should be imported wholesale into the border search context, Pls. Br. 20.

No court before or after *Riley* has accepted that position, and many have explicitly rejected it. *United States v. Cano*, 934 F.3d 1002, 1015 (9th Cir. 2019) ("post-*Riley*, no court has required more than reasonable suspicion to justify even an intrusive border search"); *United States v. Wanjiku*, 919 F.3d 472, 481, 483-84 (7th Cir. 2019) ("no circuit court, before or after *Riley*, has required more than reasonable suspicion for a border search of cell phones or electronically-stored data"); *United States v. Kolsuz*, 890 F.3d 133, 147 (4th Cir. 2018) ("Even as *Riley* has become familiar law, there are no cases requiring more than reasonable suspicion for forensic cell phone searches at the border."); *United States v. Molina-Isidoro*, 884 F.3d 287, 291-92 (5th Cir. 2018) ("For border searches both routine and not, no case has required a warrant. * * * [I]t is

telling that no post-*Riley* decision issued either before or after this search has required a warrant for a border search of an electronic device."); *United States v. Vergara*, 884 F.3d 1309, 1312 (11th Cir. 2018) ("The forensic searches of Vergara's phones required neither a warrant nor probable cause.").

These courts have rejected plaintiffs' arguments for good reason. *Riley* addressed a search in the domestic interior. But "searches of persons or packages at the national border rest on different considerations and different rules of constitutional law from domestic regulations." *United States v. Montoya de Hernandez,* 473 U.S. 531, 537 (1985). At the international border "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith," *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004), while a person's "expectation of privacy [is] less at the border than in the interior," meaning that "the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is * * * struck much more favorably to the Government at the border," *Montoya de Hernandez,* 473 U.S. at 539-40. *See United States v. Boumelhem*, 339 F.3d 414, 423 (6th Cir. 2003) (explaining that travelers have a reduced expectation of privacy when leaving the United States "if for no other reason than the departure from the United States is almost invariably followed by an entry into another country which will likely conduct its own border search"). As a result, "[r]outine searches of the persons and effects of entrants [at the border] are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *Montoya de Hernandez,* 473 U.S. at 538.

Accordingly, *Riley*'s holding for domestic searches of cell phones does not apply to a border search.

Because a person's expectation of privacy is much lower at the border, courts have required, at most, reasonable suspicion for even the most intrusive searches. Customs officials required no more than reasonable suspicion where a person was "detained incommunicado for almost 16 hours," in a manner that "was long, uncomfortable, indeed, humiliating," *Montoya de Hernandez*, 473 U.S. at 542, 544, and this Court has held that even for "strip-searches and body-cavity searches * * * the 'reasonable suspicion' standard applies," *United States v. Braks*, 842 F.2d 509, 512-14 (1st Cir. 1988). *Accord United States v. Alfaro-Moncada*, 607 F.3d 720, 729 (11th Cir. 2010) (strip search or an x-ray examination); *United States v. Seljan*, 547 F.3d 993, 1003 (9th Cir. 2008) (strip search or body cavity search); *United States v. Whitted*, 541 F.3d 480, 485-86 (3d Cir. 2008) (body cavity searches, strip searches, and x-ray examinations); *United States v. Charleus*, 871 F.2d 265, 267 (2d Cir. 1989) (body cavities searches or strip searches); *United States v. Oyekan*, 786 F.2d 832, 837-38 (8th Cir. 1986) (strip searches and involuntary x-rays); *United States v. Carter*, 590 F.2d 138, 139 (5th Cir. 1979) (strip search). Plaintiffs' argument would implausibly subject the border search of an electronic device to more demanding constitutional standards than a highly-intrusive border search involving physical contact and exposure of a person's intimate and private body parts, and would compel a heightened Fourth Amendment probable-cause-and-warrant requirement that has never before been imposed in the

border search context. Indeed, their argument effectively asks this Court to carve out a unique rule for electronic devices – a rule that does not apply to any other property or even to the search of a person's body – under which such a border search is treated no differently from the same search in the domestic interior. Plaintiffs provide no support in logic or precedent for that outcome.

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

In its Opening Brief (at 19-35), the Government explained that the CBP and ICE Directives comply with any applicable Fourth Amendment requirement for heightened suspicion in a border search of an electronic device. All three appellate courts that have addressed the issue hold that basic searches of electronic devices at the border do not require suspicion. *United States v. Touset*, 890 F.3d 1227, 1229 (11th Cir. 2018) ("no suspicion is necessary to search electronic devices at the border"); *United States v. Cotterman*, 709 F.3d 952, 960-61 (9th Cir. 2013) (en banc) ("quick look and unintrusive search of [a] laptop" is permissible "even without particularized suspicion"); *United States v. Ickes*, 393 F.3d 501, 505-08 (4th Cir. 2005). And this Court in *United States v. Molina-Gomez*, 781 F.3d 13, 17, 20 (1st Cir. 2015) – decided just nine months after *Riley* – did not suggest any constitutional difficulty with a suspicionless border search of text messages on a cell phone. While the Fourth and Ninth Circuit would require heightened suspicion for a far more comprehensive forensic search, *United States v. Kolsuz*, 890 F.3d 133, 144-48 (4th Cir 2018); *Cotterman*, 709 F.3d at 962-

67, the agencies' Directives comply with any such requirement by requiring reasonable suspicion for an advanced search in which officers connect external equipment to review, copy and/or analyze the contents of an electronic device.

Plaintiffs do not dispute that the Fourth, Ninth, and Eleventh Circuits all hold that no suspicion is required for a basic search. Nor do plaintiffs dispute that the Fourth and Ninth Circuits require heightened suspicion only for forensic searches. Nor, finally, do plaintiffs dispute that the Directives' distinction between basic and advanced searches aligns, for all practical purposes, with those courts' distinction between manual and forensic searches. *See* Govt Br. 28-35. In short, plaintiffs do not dispute that the agencies' Directives fully comply with any Fourth Amendment reasonable suspicion requirement imposed by the three appellate courts that have squarely addressed this issue.

Rather, plaintiffs argue that "any distinction" between basic and advanced searches "lacks practical significance and is therefore legally untenable," Pls. Br. 46, and as a result, any applicable reasonable suspicion standard should extend to basic searches as well as advanced searches. That argument lacks merit.

A manual or basic search is a "cursory review," "a quick look and unintrusive search," or a "relatively simple search," in which officers "turn[] on the devices and open[] and view[] image files." *Cotterman*, 709 F.3d at 957, 960 & n.6. A forensic search, by contrast, uses "a powerful tool capable of unlocking password-protected files, restoring deleted material, and retrieving images viewed on web sites," *Cotterman*,

709 F.3d at 957, with the ability to access "deleted files" that "cannot be seen or accessed by the user without the use of forensic software," *id.* at 958 n.5, resulting in a search that can be "comprehensive and intrusive [in] nature," which "cop[ies] the hard drive and then analyze[s] it in its entirety, including data that ostensibly has been deleted," *id.* at 962, in order to "mine every last piece of data on their devices," and make a "thorough and detailed search of the most intimate details" stored on those devices, *id.* at 967-68. *Cotterman* saw a "commonsense differentiation" between a manual search in which officers view a few photos, 709 F.3d at 957-58, and a comprehensive forensic examination that "transform[s]" a search "into something far different," *id.* at 961, 968. And the Fourth Circuit likewise distinguished between "a 'manual' search" in which officers "scroll through * * * recent calls and text messages," *Kolsuz*, 890 F.3d at 139, and "sophisticated forensic search methods," *id.* at 146 n.5, which "extract data from electronic devices, and conduct[] an advanced logical file system extraction," "yield[ing] an 896–page report that included [the defendant's] personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of [his] physical location down to precise GPS coordinates," *id.* at 139. While a basic search may reveal metadata, or take advantage of a device's native search function to locate files or information, Addendum 30; Pls. Br. 9, 21, 47, those rudimentary tools are worlds apart from the sophisticated and comprehensive data extraction and analysis techniques that can be utilized in an advanced forensic search.

Plaintiffs argue that basic and advanced searches differ only in the "equipment used to perform the search and certain types of data that may be accessed with that equipment." Pls. Br. 47. But plaintiffs' description fails to recognize the significant differences between the potential scope and reach of the two types of searches, differences that explain why even those courts that have required reasonable suspicion for comprehensive forensic searches have declined to do so for manual or basic searches.

First, basic and advanced searches do indeed access different "types of data." As the district court explained, a basic search is limited to "access[ing] content from the allocated space physically present on the device," Addendum 30, while an advanced search "also may be able to uncover deleted or encrypted data," Addendum 33, that cannot be accessed by a basic search. *Cotterman* identified as a critical feature of a forensic search its ability to "restor[e] deleted material," 709 F.3d at 957, including "deleted files" that "cannot be seen or accessed by the user without the use of forensic software," *id.* at 958 n.5. That difference alone sets an advanced search apart from a basic one, and demonstrates why plaintiffs and the district court are wrong to assert that "any distinction" between the two types of searches "lacks practical significance." Pls. Br. 45.[1]

[1] Although CBP's Directive specifies that both basic and advanced searches are limited to "only the information that is resident upon the device" and officers "may not intentionally use the device to access information that is solely stored remotely,"

Second, while plaintiffs are correct, in a sense, that basic and advanced searches "differ" "in the equipment used to perform the search," Pls. Br. 47, their minimization of the equipment's significance widely misses the mark. An abacus and a microprocessor differ only in the equipment used to perform mathematical calculations, but no one would claim that the two methods are comparable. The same is true for different methods of searching electronic devices. A basic search requires no heightened suspicion – as three appellate courts have concluded – in part because a search using conventional, manual methods is no more intrusive than many other border searches falling well within the category of routine border searches for which no suspicion is required. By contrast, some courts have required a heightened standard of suspicion where the "equipment" used to conduct a border search of an electronic device permits officers to comprehensively copy and analyze all data stored on an electronic device to compile an extensive record of details about a person – a record unavailable to an officer who engages only in a manual interaction with a device. *See California v. Ciraolo*, 476 U.S. 207, 215 n.3 (1986) (observations "may become invasive * * * through modern technology which discloses to the senses those

---

Addendum 55 § 5.1.2; Govt Br. 34 n.15, plaintiffs suggest that border searches of devices may nonetheless include cloud-based content, Pls. Br. 47 n.10. But the district court made no such finding, and its opinion was not predicated on such an assertion. Moreover, plaintiffs do not allege that searches of *their* devices included cloud-based content, but only that it "may have" occurred in "some" cases, and even that assertion is based solely on the fact that certain CBP record-keeping forms failed to include an affirmative indication that the device's data connection was disabled before the search. App. 135 ¶ 76.

intimate associations, objects or activities otherwise imperceptible to police or fellow citizens").

Courts frequently and properly take into account, in their Fourth Amendment analysis, the Government's use of technology and equipment to enhance their ability to conduct searches or surveillance. In *Kyllo v. United States*, 533 U.S. 27 (2001), for example, the Court held that the use of a thermal imaging device on a home, which "detect[s] infrared radiation * * * which is not visible to the naked eye," *id.* at 29, constitutes a Fourth Amendment search, *id.* at 34-35. In reaching that conclusion, the Court distinguished an officer's "warrantless visual surveillance of a home" which is "no 'search' at all," *id.* at 32, from an officer who "engage[s] in more than naked-eye surveillance" by using "technological enhancement" that reveals something beyond "ordinary perception," *id.* at 33. What "outside observers might be able to perceive, without technology" is "quite irrelevant" to what they could achieve with it, *id.* at 35 n.2, because the "modern technology reveal[s]" information that is "otherwise-imperceptib[le]" in its absence, *id.* at 38 n.5. That is why, for instance, detecting heat emanating from the home "by observing snowmelt on the roof" is different in kind from the use of a thermal-imaging device that more precisely "reveals the relative heat of various rooms in the home" and thereby reveals "information regarding the interior of the home." *Id.* It "would be foolish," the Court observed, "to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Id.* at 33-34.

Similarly, although police may, without a warrant, conduct ordinary surveillance to observe and track an automobile traveling on public streets, *United States v. Knotts*, 460 U.S. 276, 281-82 (1983), such actions may be distinguished from "GPS monitoring [to] generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," even if "the fruits of GPS monitoring" could conceivably be obtained "through lawful conventional surveillance techniques," *United States v. Jones*, 565 U.S. 400, 415-16 (2012) (Sotomayor, J., concurring). Likewise, in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the Court noted that no Fourth Amendment search occurs when officers use a pen register – a device of "limited capabilities" that records only "the outgoing phone numbers dialed on a landline telephone," *id.* at 2216, 2219, but distinguished that technology from the collection of cell-site location information that provides "a detailed and comprehensive record of the person's movements," *id.* at 2217, including "an all-encompassing record of the holder's whereabouts" with "time-stamped data" providing "an intimate window into a person's life, revealing * * * his particular movements" and which "follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales," *id.* at 2217-18. The Court reasoned that it must take into account "innovations in surveillance tools," and "seismic shifts in digital technology," because "[t]here is a world of difference between the limited types of personal information" that may be revealed by a pen

register and "the exhaustive chronicle of location information casually collected by wireless carriers today." *Id.* at 2214, 2219.[2]

Plaintiffs nonetheless argue that the "invasiveness of basic searches" could be equivalent to that of an advanced search – and they should therefore be treated the same for Fourth Amendment purposes – because officers conducting a basic search could conceivably "spend hours, days, or weeks going through the information on a device in great detail, viewing and recording it [by hand], without ever connecting it to external equipment." Pls. Br. 48-49. But as explained in the Government's Opening Brief (at 32, 36), plaintiffs' suggestion is a fanciful scenario divorced from reality, which fails to account for practical considerations of the agencies' limited manpower and resources. On a typical day,[3] CBP is responsible for inspecting and establishing the admissibility of over 1 million travelers and over $7.5 billion worth of imported products, App. 230 ¶ 33, and plaintiffs' conjecture that hordes of border officers

[2] The use of technology does not, in and of itself, alter the Fourth Amendment analysis, where it does not "reveal information * * * that would not have been visible to the naked eye," such as the use of a searchlight at night, *United States v. Knotts*, 460 U.S. 276, 285 (1983), or the "rudimentary tracking facilitated by [a] beeper," *Carpenter v. United States*, 138 S. Ct. 2206, 2215 (2018).

[3] At present, the number of travelers processed by CBP daily has decreased significantly due to issues related to COVID-19, including travel restrictions. The information in this brief regarding typical processing numbers does not reflect or account for the present decrease associated with COVID-19.

would, with pen and paper in hand, exhaustively catalogue the data in an electronic device bears no relationship to the real world.[4]

Plaintiffs contend that such "practical considerations" are "irrelevant" to the analysis. Pls. Br. 48. But "[p]ractical considerations – namely, limited police resources" often inform Fourth Amendment considerations. *Illinois v. Lidster*, 540 U.S. 419, 426 (2004). Society's reasonable expectations of privacy themselves take into account the fact that "law enforcement agents and others would not – and, indeed, in the main, simply could not" engage in "monitor[ing] and catalog[ing]" of information about an individual "for a very long period." *Jones*, 565 U.S. at 430 (Alito, J., concurring). Indeed, "the greatest protections of privacy" may be "neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken." *Id.* at 429.

Moreover, neither plaintiffs' complaint nor their statement of undisputed material facts alleges anything that even comes close to an officer who "spend[s]

[4] Plaintiffs also argue the opposite point: that an advanced search could be the equivalent of a basic search if, despite connecting external equipment, officers conduct something less than a comprehensive copying or analysis of all data on a device. Pls. Br. 48. But that possibility does not present a Fourth Amendment problem. As explained in the Government's Opening Brief (at 34 n.15), there may be searches that qualify as advanced (because an officer connects external equipment to copy or analyze data) yet an officer conducts only a modest or less-than-comprehensive analysis. But in that case the agencies' Directives would still treat that search as an advanced search requiring reasonable suspicion. Thus, at most, plaintiffs' example would be an instance in which the agencies' Directives would provide *more* protection than the Fourth Amendment might itself require.

hours, days, or weeks going through the information on a device in great detail, viewing and recording it [by hand], without ever connecting it to external equipment." Pls. Br. 49. Rather, as noted in the Government's Opening Brief (at 7-8, 34), plaintiffs provide only the sparsest descriptions of their searches, largely labeling them simply as "searches," or describing them as "manual" or "basic" without significant elaboration. If, one day, there exists a border officer who spends his days taking comprehensive hand-written notes on "hundreds of gigabytes of data," Pls. Br. 48, this Court can resolve the matter at that time, but that scenario is not remotely raised in this case by these ten plaintiffs.

Plaintiffs respond that "[i]t is inappropriate to consider the invasiveness of basic searches * * * on a case-by-case basis," Pls. Br. 49, but "[b]ecause the test of reasonableness under the Fourth Amendment is not capable of precise definition or mechanical application * * * its proper application requires careful attention to the facts and circumstances of each particular case * * * ." *Graham v. Connor*, 490 U.S. 386, 396 (1989). Accordingly, courts deciding Fourth Amendment questions often leave for another day the consideration of aberrant, unusual, or extreme fact patterns, or even just facts not presented in the case before it. For example, in *Knotts*, 460 U.S. at 281-82, the Court held that visual surveillance of a person traveling on public streets was not a search under the Fourth Amendment, because a person has no reasonable expectation of privacy in his movements from one place to another. In response to the respondent's argument that "the result of the holding" would be to

permit "twenty-four hour surveillance of any citizen of this country * * * without judicial knowledge or supervision," the Court noted that "reality hardly suggests [such] abuse," and that "if such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id.* at 283-84. Similarly, in *Carpenter* the Court held accessing seven days of cell-site location information (CSLI) constituted a search under the Fourth Amendment, but specifically declined to decide "whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be." 138 S. Ct. at 2217 n.3. "[W]e do not begin to claim all the answers today," the Court noted, "and therefore decide no more than the case before us." *Id.* at 2220 n.4.

Nor is such an approach inconsistent with the need to give officers clear constitutional guidance. The agencies' Directives not only comply with any applicable Fourth Amendment requirements of heightened suspicion for a border search of an electronic device, but include clearly delineated categories of basic and advanced searches defined by the easily-identifiable criteria of whether the device is connected to external equipment in order to review, copy, and/or analyze its contents. The Directives therefore provide adequate and clear guidance that covers the vast majority of cases, even if this Court leaves open whether the Directives would meet Fourth Amendment requirements in the highly improbable and aberrant event that a border

officer conducted the equivalent of a forensic examination by hand, using no external equipment connected to the device.

Finally, plaintiffs argue that basic and advanced searches should be treated alike because they might "access the same files." Pls. Br. 48. But the fact that two different searches reveal the same information does not mean that the Fourth Amendment necessarily treats those searches alike. "The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment. The police might, for example, learn how many people are in a particular house by setting up year-round surveillance; but that does not make breaking and entering to find out the same information lawful." *Kyllo*, 533 U.S. at 35 n.2. Similarly, the fact that a *Terry*-stop pat-down and a full strip search might both reveal the same hidden weapon does not mean that the Fourth Amendment treats those searches the same. And with reference to border searches, the relevant question under this Court's own precedents is whether the search is routine or non-routine, which turns on "[t]he degree of invasiveness or intrusiveness associated with any particular type of search." *United States v. Braks*, 842 F.2d 509, 511 (1st Cir. 1988). The fact that two different border searches of the same electronic device might access the same file does not answer that question. An officer who conducts a basic search by scrolling through a few photos or texts may come across the "same file" as an officer who conducts an advanced search that copies and analyzes hundreds of gigabytes stored on the same device, but that minimal overlap

does not mean that the two searches must necessarily be treated the same under the Fourth Amendment.

II. THE BORDER SEARCH EXCEPTION EXTENDS TO SEARCHES FOR EVIDENCE OF BORDER-RELATED OFFENSES

The border-search exception is grounded in "the longstanding right of the sovereign" to "prevent[] the entry of unwanted persons and effects," *Flores-Montano*, 541 U.S. at 152, and "to prevent the introduction of contraband into this country," *Montoya de Hernandez*, 473 U.S. at 537. Plaintiffs contend that searching an electronic device for "*evidence* of contraband" is "not sufficiently tethered to the purposes of preventing the entry of inadmissible goods and persons," Pls. Br. 24, 28, and thus such a search (in their view) "is outside the scope of the narrow purposes of the border-search exception," Pls. Br. 36.

As the Government noted in its Opening Brief (at 46-47), the Fourth Circuit rejected exactly this argument in *Kolsuz*, 890 F.3d at 143-44, explaining that "[t]he justification behind the border search exception is broad enough to accommodate not only the direct interception of contraband as it crosses the border, but also the prevention and disruption of ongoing efforts to export contraband illegally, through searches initiated at the border," and therefore permits a cell phone search "conducted at least in part to uncover information about an ongoing transnational crime." *See also United States v. Aigbekaen*, 943 F.3d 713, 721 (4th Cir. 2019) ("the Government must have individualized suspicion of an offense that bears some nexus

to the border search exception's purposes of protecting national security, collecting duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband"). Other circuits have likewise held or indicated the border search exception permits searches for non-contraband evidence of border-related offenses. *See United States v. Gurr*, 471 F.3d 144, 149 (D.C. Cir. 2006); *United States v. Fortna*, 796 F.2d 724, 738-39 (5th Cir. 1986). Although a panel of the Ninth Circuit reached a different conclusion in *United States v. Cano*, 934 F.3d 1002, 1016-18 (9th Cir. 2019), six judges recently dissented from the denial of rehearing *en banc* on this issue. *See United States v. Cano*, --- F.3d ----, 2020 WL 5225702 at *8 (9th Cir. 2020) (Bennett, J., dissenting from denial of rehearing *en banc*).

Plaintiffs' proposed distinction between a search for contraband and a search for evidence of contraband, makes no sense with respect to the purposes of the border search exception. The Government's interest in controlling its own border and preventing harmful contraband from entering the country is served not only by a search for contraband itself, but also by a search for evidence of schemes to smuggle contraband. Thus, for example, the search of a device may lead to text messages revealing that a person is, at that moment, attempting to smuggle contraband across the border, attempting to avoid the payment of duties on items procured abroad, attempting to fraudulently enter the United States in violation of the Immigration and Nationality Act, attempting to enter the United States to engage in transnational criminal activity or to engage in an action on behalf of a Foreign Terrorist

Organization, or evidence of any other border-related offense. *See, e.g., United States v. Molina-Gomez*, 781 F.3d 13, 20 (1st Cir. 2015) (noting that text messages found on defendant's phone contributed to reasonable suspicion he was smuggling drugs); *Cano*, 2020 WL 5225702 at *2 (Bennett, J., dissenting for denial of rehearing *en banc*) ("searching a traveler's cell phone at the border" may uncover "evidence of terrorist acts the traveler is about to commit in the United States; evidence the traveler is entering the United States under a false name; evidence of contemporaneous smuggling activity by the traveler; evidence of other border related crimes"). Either way, the search allows border officers to interdict contraband before it enters the country, or to otherwise enforce applicable provisions that regulate who or what may cross the border. Plaintiffs argue that uncovering evidence "indicating that the traveler was, is, or will be smuggling physical contraband" is outside the scope of the border-search exception, Pls. Br. 53, but they never explain why searching for evidence that could lead officers to interdict an attempt to smuggle contraband is untethered to the Government's interest in "prevent[ing] the introduction of contraband into this country." *Montoya de Hernandez*, 473 U.S. at 537.

Plaintiffs rely on *Boyd v. United States*, 116 U.S. 616, 623 (1886), which distinguished between "[t]he search for and seizure of stolen or forfeited goods, or goods liable to duties and concealed to avoid the payment thereof," and "a search for and seizure of a man's private books and papers for the purpose of * * * using them as evidence against him." But as the Government explained in its Opening Brief (at

41-42), the Supreme Court overruled *Boyd*'s distinction in *Warden v. Hayden*, 387 U.S. 294 (1967). *See also Cano*, 2020 WL 5225702 at *8 (Bennett, J., dissenting for denial of rehearing *en banc*) ("In *Hayden*, the Supreme Court rejected the distinction between evidence and contraband created by *Boyd*.").

Plaintiffs mistakenly contend that *Boyd* is still good law. Pls. Br. 32-35. They first argue that "*Boyd*'s discussion of the government's customs enforcement authority" "remains important." Pls. Br. 33. But that is beside the point: *Hayden* overruled *Boyd*'s distinction between a search for contraband itself and a search for evidence of contraband, and the fact that *Boyd* correctly recited the history of customs statutes has no bearing on that question.

Plaintiffs next argue that *Hayden* overruled *Boyd*'s distinction only "in the context of search warrants," Pls. Br. 33, suggesting that the distinction remains good law "in the context of a *warrant exception*," Pls. Br. 34, such as the border-search exception. But that cannot possibly be so, since *Hayden* itself was decided in the context of a warrant exception, namely exigent circumstances. *Hayden*, 387 U.S. at 298 ("[N]either the entry without warrant to search for the robber, nor the search for him without warrant was invalid" because "the exigencies of the situation made that course imperative.").[5]

[5] Indeed, *Hayden* framed the question presented as whether *Boyd*'s distinction was valid "either under the authority of a search warrant or during the course of a search incident to arrest," 387 U.S. at 296, and although the Court ultimately relied on

Moreover, *Hayden*'s rejection of *Boyd* was phrased in the broadest of terms applicable to the whole of the Fourth Amendment, not just to the context of search warrants. The Court unequivocally stated: "We today reject the distinction" "made by some of our cases between seizure of items of evidential value only and seizure of instrumentalities, fruits, or contraband," because that distinction was "based on premises no longer accepted as rules governing the application of the Fourth Amendment." *Hayden*, 387 U.S. at 300-01. To begin with, the distinction lacks any grounding in constitutional text: "Nothing in the language of the Fourth Amendment supports the distinction between 'mere evidence' and instrumentalities, fruits of crime, or contraband," because the text speaks of the "'right of the people to be secure in their persons, houses, papers, and effects * * * ,' without regard to the use to which any of these things are applied. This 'right of the people' is certainly unrelated to the 'mere evidence' limitation." *Id.* at 301. Nor does *Boyd*'s distinction makes sense in light of Fourth Amendment privacy interests: "Privacy is disturbed no more by a search directed to a purely evidentiary object than it is by a search directed to an instrumentality, fruit, or contraband," and "nothing in the nature of property seized as evidence renders it more private than property seized, for example, as an instrumentality; quite the opposite may be true." *Id.* at 301-02. Moreover, *Boyd*'s

---

the exigent circumstances rather than on a search incident to arrest, *id.* at 298-99, the Court clearly understood that its overruling of *Boyd* extended beyond the context of a search warrant.

distinction is "wholly irrational" and unworkable, because "depending on the circumstances, the same 'papers and effects' may be 'mere evidence' in one case and 'instrumentality' in another." *Id.* at 302.[6] Finally, *Boyd*'s distinction rested on the "premise that property interests control the right of the Government to search and seize," but modern Fourth Amendment cases "recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts." *Id.* at 304. Accordingly, the Court held, "there is no viable reason to distinguish intrusions to secure 'mere evidence' from intrusions to secure fruits, instrumentalities, or contraband." *Id.* at 310. Nothing in *Hayden*'s holding or reasoning limits its repudiation of *Boyd* to the context of search warrants.

Plaintiffs also rely (Pls. Br. 34) on Judge Costa's concurring opinion in *United States v. Molina-Isadoro*, 884 F.3d 287 (5th Cir. 2018), which opined that "there are reasons to believe [*Boyd*'s] distinction still matters when it comes to border searches," *id.* at 296 n.7. Specifically, Judge Costa stated that even after *Hayden*, "the Supreme

[6] For example, plaintiffs agree that under the border-search exception, officers may "inspect[] official documents such as passports and visas," Pls. Br. 40, but what are those documents if not *evidence* of admissibility and thus evidence of a possible border-related offense? *See United States v. Martinez-Fuerte,* 428 U.S. 543, 558 (1976) (where officers conduct seizure under Fourth Amendment during a border check operation, officers may permissibly require "the production of a document evidencing a right to be in the United States"). And *Cano* agreed that child pornography is *both* "contraband subject to seizure at the border" and "is *also* evidence of various crimes," 934 F.3d at 1017, demonstrating that the supposed distinction between contraband and evidence is illusive at best, and unworkable at worst.

Court has continued to chiefly rely on the detection-of-contraband rationale in supporting the government's broad border-search authority." *Id.* But as explained above, the Government's interest in detecting contraband is equally served by a search for evidence of a scheme to smuggle contraband as it is by a search for the contraband itself, because both searches allow border officers to interdict contraband before it crosses the border. *Cf. Hayden*, 387 U.S. at 306 n.11 ("the prevention of crime is served at least as much by allowing the Government to identify and capture the criminal, as it is by allowing the seizure of his instrumentalities"). Judge Costa also reasoned that "*Hayden* rejected [*Boyd*'s] distinction as one based on a 'discredited' property view of the Fourth Amendment, but that approach is enjoying a resurgence." *Id.* (citing *Florida v. Jardines*, 569 U.S. 1, 5 (2013), and *United States v. Jones*, 565 U.S. 400, 404–05 (2012)). But *Hayden* rejected *Boyd*'s "premise that property interests *control* the right of the Government to search and seize," 387 U.S. at 304 (emphasis added), and the very cases Judge Costa cited agree that "property rights are not the sole measure of Fourth Amendment violations," *Jardines*, 569 U.S. at 5, and that the Supreme Court has "deviated from that exclusively property-based approach," *Jones*, 565 U.S. at 405. *See Byrd v. United States*, 138 S. Ct. 1518, 1526 (2018) ("Expectations of privacy protected by the Fourth Amendment, of course, need not be based on a common-law interest in real or personal property" and privacy expectations "supplement[], rather than displace[] the traditional property-based understanding of the Fourth Amendment"); *Carpenter*, 138 S. Ct. at 2214 n.1. Moreover, *Hayden* rejected *Boyd* not

merely because the evidence/contraband distinction was premised on the discredited view that property rights control the Fourth Amendment analysis, but also because the distinction lacked textual support in Constitution; was irrational and unworkable; and made no sense with respect to the interests of personal privacy.

Plaintiffs likewise rely (Pls. Br. 37) on Judge Costa's concurring view that "it is uncertain whether the evidence-gathering justification is so much stronger at the border that it supports warrantless and suspicionless searches of the phones of the millions crossing it." *Molina-Isadoro*, 884 F.3d at 296. But that reasoning gets the analysis backwards: Because *Hayden* rejected *Boyd*'s distinction between a search for contraband and the search for evidence of contraband, officers do not need to have a higher "justification" when they search for evidence of contraband than they do when they search for contraband itself. Thus, the question is not whether the Government can show that the "evidence-gathering justification is so much stronger at the border," but whether plaintiffs can show that there is something unique about the border compelling this Court, in that context alone, to revive *Boyd*'s atextual and unworkable distinction. Neither plaintiffs nor Judge Costa give any reason for doing so.

In addition, *Boyd*'s distinction – as applied to border searches of electronic devices by the Ninth Circuit in *Cano* – makes little sense in practical application. First, consider *Cano*'s treatment of basic searches. In *Cano*, border officers had plenty of suspicion that the defendant was smuggling drugs: a drug-detecting dog alerted to his vehicle, and the ensuing search revealed 14 kilograms of cocaine. 934 F.3d at 1008.

But officers had no reason to suspect that the defendant was smuggling digital contraband: "the record does not give rise to any objectively reasonable suspicion that the digital data in the phone contained contraband." *Id.* at 1021. Nonetheless, the officers conducted a basic search of the defendant's cell phone, looking at the phone log and text messages, conceding that they did so for the purpose of finding leads in the drug smuggling case. *Id.* at 1008. Yet *Cano* held that the officer's "observation" and "accessing" of text messages and phone log, even "without any suspicion whatsoever," was "beyond dispute" and "falls comfortably within the scope of a search for digital contraband." *Id.* at 1019. The court reasoned that because digital contraband such as child pornography "may be sent via text message" and "[c]riminals may hide contraband in unexpected places," it was "reasonable for the [] officers to open the phone's call log to verify that the log contained a list of phone numbers and not surreptitious images or videos." *Id.*

Cano did not explain, however, how judges (or border officers) are supposed to decide where criminals "may" hide digital contraband in an electronic device and where they may not. Are courts to make that determination on an app-by-app basis, file-by-file, or byte-by-byte? That question is further complicated by the fact that for many electronic devices, "[e]ven the most conventional 'files' * * * are not maintained, like files in a file cabinet, in discrete physical locations separate and distinct from other files. They are in fact 'fragmented' on a storage device, potentially across physical locations * * * . [R]arely will one file be stored intact in one place on a hard drive; so-

called 'files' are stored in multiple locations and in multiple forms." *United States v. Ganias*, 824 F.3d 199, 213 (2d Cir. 2016) (en banc); *see Cotterman*, 709 F.3d at 965 (officers found child pornography "in the unallocated space of Cotterman's laptop, the space where the computer stores files that the user ostensibly deleted"). Thus, in practical application, *Cano*'s treatment of where or what officers may access or examine in the course of a basic search is uncertain and ill-defined.[7]

Cano's implications are even more illogical if that decision is interpreted broadly, as Judge Bennett suggested in his dissent from the Ninth Circuit's denial of rehearing en banc. Broadly construed, that rule could lead to an odd and irrational result, namely, that an officer who *does* have reasonable suspicion that a traveler is committing all kinds of border-related offenses – for example, an officer "armed with reasonable suspicion the phone contains evidence of terrorist acts the traveler is about to commit in the United States; evidence the traveler is entering the United States under a false name; evidence of contemporaneous smuggling activity by the traveler;

[7] *Cano* did impose one limit on a basic search, but it did not relate to where or what officers may observe or access. *Cano* held that whatever officers may observe or access during a basic search of an electronic device, they may not take notes on, or photograph, what they see unless it is digital contraband, for doing so (in *Cano*'s view) "has no connection to ensuring that the phone lacks digital contraband." *Id.* at 1019. Or, to be more precisely, *Cano* holds that the officers may not take notes or photographs in reliance on the border search exception, but left open whether such conduct would be permissible under the plain view exception, or whether such actions would constitute harmless error where the same notes would be available by alternative means such as third-party phone records. *Id.* at 1009 n.1, 1019 n.11.

[or] evidence of other border related crimes" – is "constitutionally barred" from conducting an advanced search of the device at the border based on the border search exception. *Cano*, 2020 WL 5225702 at *2 (Bennett, J., dissenting for denial of rehearing en banc). Unless that officer has reasonable suspicion that the device contains child pornography or other digital contraband, an advanced border search is constitutionally out of bounds. While the touchstone of the Fourth Amendment is "reasonableness," "such distinctions make no sense" and "cannot possibly be reasonable." *Id.* at *8.[8]

In the end, although plaintiffs attempt to breathe new life into *Boyd*'s distinction between contraband and evidence, they endorse neither its holding nor its rationale. As recognized by both the district court, Addendum 21-22, and *Cano*, 934 F.3d at 1007, even applying *Boyd*'s distinction would, at a minimum, permit border officers to search electronic devices for digital contraband, such as child pornography, electronic

[8] While *Cano* addresses the scope of the border search exception with respect to the intervention of contraband, the Government does not construe *Cano* as addressing other recognized reasons for the border search exception, such as helping to determine the admissibility of travelers or national security concerns, and thus the Government does not construe *Cano* as foreclosing reliance on those other grounds to sustain border searches of electronic devices in appropriate circumstances. The district court in this case likewise did not reach those grounds. *See* Govt Br. 40-41 n.18. Plaintiffs contend that the district court did reject a search of an electronic device for evidence of admissibility, *see* Pls. Br. 40, but in fact the district court had no need to address that question because plaintiffs in this case are U.S. citizens or lawful permanent residents who by definition are admissible, Addendum 21-22. And contrary to plaintiffs' contention, Pls. Br. 51 n.13, neither the district court's declaratory judgment nor its injunctive order addressed national security reasons that might support a border search of an electronic device, *see* Govt Br. 10 n.9.

material that violates intellectual property rights, or classified information on an unauthorized device. But plaintiffs argue that even *that* kind of search is impermissible under the border-search exception, Pls. Br. 37-39, demonstrating that they do not genuinely seek to reimpose *Boyd*'s holding at all, but simply ask this Court to create a rule (coming from nowhere, based on no precedent) that electronic devices are wholly exempt from the border-search exception regardless of whether the search is for contraband or evidence. Nor, for that matter, do plaintiffs endorse *Boyd*'s underlying rationale, which rested on the notion that property interests control the Fourth Amendment analysis. Plaintiffs eschew that rationale for good reason: if the Fourth Amendment analysis were defined exclusively by property rights, it would eviscerate their principal argument, which turns on expectations of privacy, not property rights.[9] As explained above, *Boyd* was unpersuasive on its own terms, but it makes even less sense for plaintiffs to repeatedly invoke that case while disclaiming both its holding and its rationale.

Finally, plaintiffs argue that exceptions to the Fourth Amendment's warrant requirement may not be designed primarily to serve a general interest in crime control. Pls. Br. 29. Plaintiffs do not dispute that a border search for contraband itself is

[9] Indeed, if Fourth Amendment rights were defined entirely by property interests it could mean that a basic search (involving a physical touching) might be entitled to Fourth Amendment protection, while an advanced search using only a wireless connection (and thus no physical touching) might be free from constitutional constraints. *See Jones*, 565 U.S. at 426-27 (Alito, J. concurring).

permissible because it is designed to prevent harmful items from entering the country, rather than serving a general interest in crime control. Pls. Br. 24-25. But the same is true when border officers search for evidence of contraband, which is equally designed to detect and interdict the contraband before it enters the country, and not to serve general crime-control interests. Plaintiffs similarly argue that the Government searches electronic devices "to seek evidence of unlawful conduct with no nexus to the admissibility of goods and people." Pls. Br. 30. But the CBP Directive at issue requires "reasonable suspicion *of activity in violation of the laws enforced or administered by CBP*, or in which there is a national security concern," Addendum 56 § 5.1.4 (emphasis added), and ICE's 2018 supplemental guidance is similar, *see* Govt. Br. at 5-6, and thus the Directives themselves limit the agencies to searching for evidence of border-related offenses, and rather than serving a wider interest in combatting crimes generally.

Plaintiffs contend that border searches necessarily serve an impermissible interest in general crime control, and not the Government's interest in stopping harmful goods from entering the country, simply because of the "wide range" of laws CBP and ICE are authorized to enforce. Pls. Br. 30. As an initial matter, this argument has nothing to do with electronic devices – if plaintiffs were correct, it would mean that border officers could not conduct *any* searches of any kind, at least with respect to the enforcement of laws deemed insufficiently related to the Government's interest in protecting the border. Regardless, on closer inspection, all

of the authorities to which plaintiffs point relate to the Government's interest in controlling the passage of goods over the border and preventing harmful items from entering (or leaving) the country, or include a border nexus of some kind.

For example, enforcement of "financial" laws, Pls. Br. 30, includes customs officials' statutory authority to conduct a warrantless search to enforce provisions relating to the transfer of $10,000 or more out of the United States, 31 U.S.C. §§ 5316-5317; *see* App. 221 ¶ 7, which is predicated on the "[l]egitimate governmental interest in the flow of currency across international borders," *United States v. Dichne*, 612 F.2d 632, 638 (2d Cir. 1979). As for "food safety" and "agricultural" laws, Pls. Br. 31, Congress has authorized the Secretary of Agriculture to prohibit, for example, "the importation or entry of any animal" as "necessary to prevent the introduction * * * of any pest or disease of livestock," 7 U.S.C. § 8303(a)(1), and "[t]he importation into the United States" of certain "agricultural or vegetable seeds," 7 U.S.C. § 1581(1), which border officers enforce pursuant to 19 C.F.R. §§ 12.8, 12.10. Congress has also enacted "intellectual property" laws, Pls. Br. 30, prohibiting the importation of articles where the U.S. International Trade Commission finds the infringement of a valid and enforceable patent or copyright, 19 U.S.C. § 1337(a)(1)(B)(i), which border officers enforce pursuant to 19 C.F.R. § 12.39. As to "vehicle emissions" laws, Pls. Br. 31, Congress prohibited the importation into the United States any new motor vehicle unless it receives a certificate of conformity that it complies with applicable vehicle emission standards, 42 U.S.C. §§ 7521, 7522, 7525, which border officers enforce

pursuant to 19 C.F.R. § 12.73. Finally, as to "tax" law, Pls. Br. 30, even plaintiffs concede that a search falls within the border-search exception if it relates to customs duties, Pls. Br. 25-26, and the customs duty is simply a tax on imported goods. *See, e.g.*, 19 C.F.R. § 148.26(a) (providing for "[t]he internal revenue tax on taxable cigars and cigarettes in a passenger's baggage" to "be paid to Customs, using the Customs entry form as a return.").

Plaintiffs are not wrong to say that border officers enforce a wide range of laws pertaining to items crossing the border – including the importation of certain cheeses, wild animals and insects, counterfeit coins, human antitoxins, sea-otter skins, and pre-Columbian architectural sculptures, to name just a few, *see* 19 C.F.R. Part 12; App. 221 ¶ 7. But the very fact that that these are goods that Congress has prohibited from crossing the border, or whose importation is regulated or restricted by statute, demonstrates that enforcement of these laws falls well within "the longstanding right of the sovereign" to "prevent[] the entry of unwanted persons and effects," *Flores-Montano*, 541 U.S. at 152, and "to prevent the introduction of contraband into this country," *Montoya de Hernandez,* 473 U.S. at 537. *See Cano*, 2020 WL 5225702 at *8 (Bennett, J., dissenting from denial of rehearing *en banc*) (noting that the sovereign's interest in border protection extends, among other things, to the "entry of terrorists and terrorist weapons," "person seeking admission to the United States," "undeclared currency flowing through the border," and other "transnational offenses involving export controls and national security interests"); *Aigbekaen*, 943 F.3d at 721 (requiring

"some nexus to the border search exception's purposes of protecting national security, collecting duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband"). It follows that border searches to enforce these provisions fall well within the purposes of the border-search exception, because they all equally serve to enforce Congress's restrictions on the goods permitted to cross the border into (or out of) this Nation.[10]

III. THE FOURTH AMENDMENT DOES NOT IMPOSE A RIGID RULE FOR THE LENGTH OF DETENTION OF ELECTRONIC DEVICES

Both CBP's and ICE's Directives specify that they may detain electronic devices for a "reasonable" period of time to conduct a border search. Addendum 58 § 5.4.1; Addendum 67 § 8.3.1. That limitation is consistent with Supreme Court precedent, which has "consistently rejected hard-and-fast time limits" on the duration

[10] Plaintiffs' description of the Government's interest in conducting border searches is also noticeably imprecise. Plaintiffs contend a search must be related "to customs and immigration enforcement," Pls. Br. 30, but a search for illegal drugs is obviously within the purpose of the border-search exception even though it is neither related to enforcing the payment of customs duties nor to immigration. Nor does it matter whether a border officer conducts a search to enforce "laws at the border on behalf of various federal agencies." Pls. Br. 31. Border officers conduct searches for illegal drugs even though "[i]mportations and exportations of controlled substances" "are governed by laws administered by the Drug Enforcement Administration of the Department of Justice," 19 C.F.R. § 161.2(a)(2). Similarly, plaintiffs argue border searches must have a "nexus to the *admissibility* of goods and people," Pls. Br. 30 (emphasis added), but "[t]he justification behind the border search exception is broad enough to accommodate not only the direct interception of contraband as it crosses the border, but also the prevention and disruption of ongoing efforts to *export* contraband illegally, through searches initiated at the border," *Kolsuz*, 890 F.3d at 143-44 (emphasis added).

of detentions, particularly at the border, because "common sense and ordinary human experience must govern over rigid criteria." *Montoya de Hernandez*, 473 U.S. at 543. In light of the agencies' Directives and Supreme Court guidance, the district court correctly declined to impose a rigid rule specifying a precise limit on the duration of time that the agencies may detain devices in order to conduct a border search.

Plaintiffs "do not dispute that duration must be reasonable," and agree that rigid rules are inappropriate, but nonetheless fault the agencies' Directives for "provid[ing] no meaningful limit on duration whatsoever." Pls. Br. 60. But plaintiffs do not explain what additional limit the Directives, or a court, could require without imposing precisely the kind of rigid time limit that is inappropriate under the Fourth Amendment. Indeed, plaintiffs repeatedly suggest an inflexible rule under which detaining an electronic devices for 12 days would necessarily be unreasonable, *see* Pls. Br. 11, 49, 60, despite this Court's conclusion in *Molina-Gomez*, 781 F.3d at 21, that CBP officers conducting a border search did not act unreasonably in detaining the defendant's electronic devices for 22 days.

Plaintiffs contend that "when the length of a seizure increases," then courts necessarily must impose "a higher standard," Pls. Br. 59. But there is no rule that when the length of a seizure or detention "increases," the Fourth Amendment scrutiny must increase in lockstep fashion. The cases upon which plaintiffs rely (Pls. Br. 59) in fact emphasize that the Fourth Amendment eschews that kind of rigid rule. *See United States v. Place*, 473 U.S. 696, 709 & n.10 (1983) ("we decline to adopt any

outside time limitation" because "[s]uch a limit would undermine the equally important need to allow authorities to graduate their responses to the demands of any particular situation"); *Molina-Gomez*, 781 F.3d at 21 ("The Supreme Court has consistently rejected hard-and-fast time limits, instead placing an emphasis on common sense and ordinary human experience.").[11]

Plaintiffs also argue that for a seizure of an item to be lawful, it must be predicated on the same level of suspicion as required for a subsequent search of the item. Pls. Br. 58. But *United States v. Place*, on which plaintiffs rely, holds the opposite. There, the Supreme Court concluded that "the initial seizure of respondent's luggage" was permitted "on the basis of reasonable, articulable suspicion," even where a subsequent search of the luggage "could not be justified on less than probable cause." 462 U.S. at 702, 706. Likewise, under certain circumstances officers may seize and secure a home if they have probable cause, even if a later search of the home would require a warrant. *Illinois v. McArthur*, 531 U.S. 326 (2001). And *Riley* noted that the defendants in that case "concede[d] that officers could have seized and secured their cell phones to prevent destruction of evidence while seeking a warrant," which the

[11] Nor is it even clear what plaintiffs mean by referring to the length of a seizure that "increases" – increases as to compared to what? Of course, if the seizure increases beyond a reasonable period of time, then by definition the seizure would be unreasonable. But that begs the question of what period of time is reasonable. And as this Court emphasized in *Molina-Gomez*, merely because a seizure takes a long time does not mean it is unreasonable under the circumstances. *See* 781 F.3d at 21 ("Though twenty-two days does seem lengthy, it is not unreasonable under these circumstances.").

Court characterized as "a sensible concession" in light of *Illinois v. McArthur*. *See Riley*, 573 U.S. at 388.

But even accepting plaintiffs' premise as correct would not advance their argument. For the reasons explained above, the agencies' Directives comply with any applicable Fourth Amendment requirement for a search of electronic devices at the border, and thus even under plaintiffs' theory, the initial detention of the devices would be permissible as well. Plaintiffs' contrary argument rests on the assumption that a search of an electronic device at the border requires a warrant and probable cause, Pls. Br. 58, which is incorrect for the reasons explained above, *supra* at 5-8.

Finally, it is worth noting that nothing in plaintiffs' arguments turns on the personal privacy interests in the data contained in their devices. Those interests may be relevant to the *search* of the device, but they have no bearing on a *seizure* of the device. Indeed, nothing in plaintiffs' arguments turns on the fact that CBP or ICE officers seized an electronic device, as opposed to luggage or any other piece of property. Nor, for that matter, is there anything in plaintiffs' arguments about the permissible length of a seizure that would be confined to the border-search context. Plaintiffs' argument, in short, would require strict time limits on the duration of any detentions, which must be specified in advance in written Directives. This Court should reject any such inflexible rule.

IV. THE FIRST AMENDMENT DOES NOT REQUIRE A HEIGHTED STANDARD FOR SEARCHES

Plaintiffs argue that where a search "reveal[s] expressive and associational activities," Pls. Br. 54, the Fourth Amendment requires "heightened scrutiny" for those searches, Pls. Br. 56.

The district court correctly rejected this argument. The court reasoned that the CBP and ICE Directives "at issue here are content-neutral," that "there is no suggestion on this developed record that Plaintiffs were targeted and investigated for their speech or associations," and that relevant Supreme Court and First Circuit precedent suggests that "a different standard for First Amendment issues from the Fourth Amendment issues is not necessarily required." Addendum 40-42. The district court also observed that even if a heightened standard applied, it would be satisfied in light of "the paramount government interests [in] the interdiction of persons and goods at the border," and because "it is not clear what less restrictive means could be employed here." Addendum 41.

In *New York v. P.J. Video, Inc.*, 475 U.S. 868 (1986), the Supreme Court addressed "the proper standard for issuance of a warrant authorizing the seizure of materials presumptively protected by the First Amendment," *id.* at 869, and rejected the view that "there is a higher standard for evaluation of a warrant application seeking to seize such things as books and films," *id.* at 871. The Supreme Court noted that it had "never held or said that such a 'higher' standard is required by the First

Amendment," and held "that an application for a warrant authorizing the seizure of materials presumptively protected by the First Amendment should be evaluated under the same standard of probable cause used to review warrant applications generally." *Id.* at 874-75. This Court has likewise held that the Fourth Amendment "assessment is no different where First Amendment concerns may be at issue," *United States v. Brunette*, 256 F.3d 14, 16 (1st Cir. 2001), and other court have likewise rejected "the proposition that a stricter probable cause standard should apply when first amendment values are implicated," *United States v. Weber*, 923 F.3d 1338, 1343 n.6 (9th Cir. 1990); *accord United States v. Syphers*, 426 F.3d 461, 465 n.1 (1st Cir. 2005) ("The assessment of probable cause is no different where First Amendment concerns may be at issue."); *White Fabricating Co. v. United States*, 903 F.2d 404, 411 (6th Cir. 1990) ("We recognize also that there is no 'higher' standard for probable cause for issuance of a warrant required in First Amendment cases such as this one.").

Two courts of appeals have similarly held that there is no heightened Fourth Amendment standard for a border search of an electronic device, even when expressive material may be involved. *United States v. Ickes*, 395 F.3d 501 (4th Cir. 2005), reasoned that imposing such a higher Fourth Amendment standard "would create a sanctuary at the border for all expressive material—even for terrorist plans," which "would undermine the compelling reasons that lie at the very heart of the border search doctrine," *id.* at 506. In addition, such a rule would be difficult to administer, forcing border agents "to decide—on their feet—which expressive

material is covered by the First Amendment," and such "legal wrangles at the border are exactly what the Supreme Court wished to avoid by sanctioning expansive border searches." *Id.*; *see Flores-Montano*, 541 U.S. at 152 ("Complex balancing tests * * * have no place in border searches of vehicles."). Finally, the court noted that in *P.J. Video* "the [Supreme] Court refused to require a higher standard of probable cause for warrant applications when expressive material is involved," and the court found "it unlikely that [the Supreme Court] would favor a similar exception to the border search doctrine." *Ickes*, 395 F.3d at 507. Accordingly, the court held "that the border search doctrine is not subject to a First Amendment exception." *Id.*

United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008), likewise reasoned that a higher Fourth Amendment standard for a border search involving expressive material would "protect terrorist communications," "create an unworkable standard for government agents," and "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." *Id.* at 1010. The court was thus "persuaded by the analysis of our sister circuit" and "follow[ed] the reasoning of *Ickes*." *Id.*

Plaintiffs' reliance (Pls. Br. 56) on *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), is misplaced. *Zurcher* held that "courts apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search," *id.* at 565, but did not hold that the Fourth Amendment standard was different or higher.

Nor does *Tabbaa v. Chertoff*, 509 F.3d 89 (2d Cir. 2007), assist plaintiffs' argument. *See* Pls. Br. 57. The court in that case "d[id] not need to reach this issue" because even assuming First Amendment scrutiny applied, the Second Circuit (like the district court in this case, Addendum 41) concluded that the border search in question "easily pass[ed] muster," *id.* at 102 n.5, noting that protecting the borders is a compelling national interest and border searches are the most effective way to do so, *id.* at 103.

Finally, it is worth observing the breadth of plaintiffs' argument. They contend that a higher Fourth Amendment standard applies whenever a search would "reveal[] expressive and associational activities." Pls. Br. 54. That argument does not turn on whether border agents search an electronic device or some other property. Thus, for example, if border officers searched a person's luggage – as plaintiffs concede they may, Pls. Br. 18, 25-26, 35 – and during the examination officers see the title of a book or DVD inside, that would presumably implicate plaintiffs' asserted First Amendment "right to read books and watch movies privately," Pls. Br. 55, triggering (in plaintiffs' view) a heightened Fourth Amendment standard. For all the reasons that argument was rejected in *Ickes* and *Arnold*, it should be rejected here as well.

V. THE DISTRICT COURT DID NOT ABUSE ITS DISCRETION IN DECLINING TO GRANT THE EQUITABLE REMEDY OF EXPUNGEMENT

A district court has a "narrow" power to "exercise its equitable discretion to expunge" records, but its "refus[al] to exercise" that authority is reviewed only for "an abuse of discretion." *Reyes v. DEA*, 834 F.2d 1093, 1098-99 (1st Cir. 1987). The

district court in this case recognized that it had the authority to award such relief, Addendum 44, but declined "in its discretion" to do so, Addendum 47. The district court, drawing on an analogy to the exclusionary rule and the good faith exception, noted that even where a search violates the Fourth Amendment, the remedy of suppression is not granted where the costs of suppression to the truth-finding process outweigh the benefits of its deterrent effect on unlawful police behavior. Addendum 44-45. By analogy, the district court reasoned, expungement is not warranted here, where the "paramount government interest" in protecting the border outweighs the interests in expungement, "particularly where the law regarding the legality of electronic device searches has been in flux," and thus any possible Fourth Amendment violation would have been made by officers acting in good faith. Addendum 45.

Plaintiffs fail to demonstrate that the district court abused its discretion in denying the equitable relief of expungement. Plaintiffs argue that courts have authority to grant such relief, Pls. Br. 60-61, but the district court did not hold otherwise. It denied relief as a matter of its discretion, not for lack of authority.

Plaintiffs also argue that that they are harmed by the continued retention of information and its possible future viewing or dissemination. Pls. Br. 62-63. But the district court took that into account in exercising its discretion. Addendum 46-47. It nonetheless concluded that expungement was not warranted considering the Government's paramount interests in protecting the border and the fact that officers

acted in good faith in an area where the state of the law has been in flux. Plaintiffs fail to show any abuse of discretion in that conclusion.

Plaintiffs further argue (Pls. Br. 62 n.16) that the district court erred in relying on cases involving the exclusionary rule. But the court did so only as an illustrative analogy, observing that in that context courts may weigh the costs of a Fourth Amendment remedy against its asserted benefits in determining whether to grant relief, and that the same may be done in the expungement context. Nothing in the court's use of that analogy amounts to an error of law or abuse of discretion.

Finally, plaintiffs' expungement argument depends, at a minimum, on the premise that the searches of their devices violated the Fourth Amendment. For the reasons discussed above and in the Government's Opening Brief, however, the CBP and ICE Directives comply with any applicable Fourth Amendment requirement. Notably, plaintiffs describe nearly all of their searches as either "basic" or "manual" – or as "searches" without any further elaboration, Govt. Br. 7-8 & nn.4-6 – and thus all such border searches were lawful even without suspicion.

While two plaintiffs – Sidd Bikkannavar and Matthew Wright – alleged an advanced or forensic search, Govt. Br. 8 & n.7, the Government did not retain any data from the latter plaintiff. *See* App. 207-208 ¶ 151.b ("Defendants aver that all copies of Wright's data have been deleted."); App. 338 ¶ 151.b ("[n]o dispute" from plaintiffs). As for plaintiff Bikkannavar, his search occurred under CBP's old policy, not its current one, and this Court would be well within its discretion to deny

expungement where granting such relief would require this Court to unnecessarily address constitutional questions it could otherwise avoid in order to adjudicate the lawfulness of a policy superseded more than two years ago.

As explained in the Government's Opening Brief (at 35), this Court can and should resolve the Fourth Amendment question of whether heightened suspicion is required to conduct a border search of an electronic device by holding that the agencies' *current* Directives comply with any applicable constitutional requirements for heightened suspicion. That approach avoids any need to resolve the differences among the Fourth, Ninth, and Eleventh Circuits with respect to whether reasonable suspicion is required for advanced searches, thereby avoiding, to the extent possible, the unnecessary resolution of constitutional questions.

But that prudent path would be disrupted if this Court were forced to adjudicate the constitutionality of CBP's now-obsolete policy, as applied in a single instance, for the sole purpose of determining whether the remedy of expungement should be granted. A court may properly decline to grant the equitable relief of expungement where doing so would first force the court to wade into and resolve a constitutional dispute, in a rapidly evolving area of the law in which courts disagree, in order to adjudicate the lawfulness of a superseded policy at the best of a single plaintiff. In such circumstances, expungement based on the Government's Fourth Amendment behavior pursuant to defunct policies the agencies no longer employ could have no deterrent effect on the Government's operations under its current

Directives. By contrast, expungement would impose costs on the Government (in destroying records) and on the courts (in unnecessarily adjudicating difficult constitutional questions relating to superseded agency policies). On balance, therefore, a court may properly decline to grant the equitable remedy of expungement in such circumstances.

Moreover, even if there were a Fourth Amendment violation in this case, that fact, standing alone, would not make it unlawful for the Government to retain the relevant materials, nor would it compel expungement of records unlawfully obtained. When a search violates the Fourth Amendment, the exclusionary rule ordinarily precludes the government from introducing the fruits of the search as part of its case in chief in a criminal proceeding against the subject of the search. But the exclusionary rule does not foreclose the government from making other uses of such evidence. To the contrary, outside of the context of criminal trials, the government is generally free to use – and hence necessarily free to retain possession of – the fruits of illegal searches. *See, e.g.*, *Pennsylvania Board of Probation & Parole v. Scott*, 524 U.S. 357, 362 (1998) (noting that the Supreme Court has continually declined to extend the exclusionary rule to proceedings other than criminal trials); *INS v. Lopez-Mendoza*, 468 U.S. 1032, 1034, 1050 (1984) (unlawfully obtained materials generally may be used against an alien in civil immigration proceedings); *United States v. Calandra*, 414 U.S. 338, 347-452 (1974) (noting that exclusionary rule "has never been interpreted to

proscribe the use of illegally seized evidence in all proceedings against all persons" and refusing to extend exclusionary rule to grand jury proceedings).

Applying these principles, the court in *Grimes v. CIR*, 82 F.3d 286 (9th Cir. 1996), "assume[d] for the sake of argument that [certain tax records were] seized illegally," *id.* at 288, but held that "[t]he IRS is entitled to keep copies of Grimes' records," *id.*at 291, reasoning "[b]ecause the government may now use illegally obtained evidence in a variety of situations, *it should be permitted to retain copies of such evidence* absent extreme circumstances not apparent from this record." *Id.* (emphasis added). *See also Ramsden v. United States*, 2 F.3d 322, 327 (9th Cir. 1993) (allowing government to retain copies of illegally obtained materials even after finding that the government had "display[ed] callous disregard for Ramsden's constitutional rights"); *Mayfield v. United States*, 599 F.3d 964, 971 (9th Cir. 2010) ("The government is correct that it would not necessarily be required by a declaratory judgment to destroy or otherwise abandon the materials. * * * [T]here is nothing in the declaratory judgment that would make it unlawful for the government to continue to retain the derivative materials."). In short, absent extreme circumstances plaintiffs fail to show here, expungement would not be required even assuming plaintiffs could establish a Fourth Amendment violation.

CONCLUSION

For the foregoing reasons and those stated in the Government's Opening Brief, this Court should reverse and remand the judgment with instructions to enter summary judgment for the Government.

Respectfully submitted,

ANDREW E. LELLING
United States Attorney

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

September 2020

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limit of Federal Rule of Appellate Procedure 32(a)(7)(B) because it contains 12,671 words. This brief also complies with the typeface and type-style requirements of Federal Rule of Appellate Procedure 32(a)(5)-(6) because it was prepared using Microsoft Word 2016 in Garamond 14-point font, a proportionally spaced typeface.

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

CERTIFICATE OF SERVICE

I hereby certify that on September 30, 2020, I electronically filed the foregoing corrected brief with the Clerk of the Court for the United States Court of Appeals for the First Circuit by using the appellate CM/ECF system. Participants in the case are registered CM/ECF users, and service will be accomplished by the appellate CM/ECF system.

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