No. 20-1505

IN THE

Supreme Court of the United States

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

Petitioners,

—v.—

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

Respondents.

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

REPLY BRIEF FOR PETITIONERS

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

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

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

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

INTRODUCTION

This case asks what the Fourth Amendment requires with respect to searches of travelers' electronic devices at the U.S. border. The government contends that this Court should decide the question of the permissible scope of such a search—i.e., whether it should be limited to digital contraband—without addressing the predicate question of what standard of suspicion the Fourth Amendment requires for a search in the first place. But to so split the question would be illogical, would fail to resolve a related split on that question, and would leave lower courts, the government, and the public guessing how to apply the Fourth Amendment's protections in this context. The Court should grant certiorari to resolve the complete Fourth Amendment question of what suspicion is required to search an electronic device at the border and what the appropriate scope of that search is. The issues are interrelated, and can and should be resolved on the basis of the robust factual record developed in this case.

I. THIS COURT SHOULD CONSIDER BOTH THE STANDARD OF SUSPICION REQUIRED FOR DEVICE SEARCHES AT THE BORDER AND THE PERMISSIBLE SCOPE OF SUCH SEARCHES.

The government asks this Court to grant certiorari in *United States v. Cano*, 934 F.3d 1002 (9th Cir. 2019), *petition for certiorari pending* (filed Jan. 29, 2021), and to hold the petition in this case. U.S. Br. 11. But doing so makes little sense. A decision on the permissible scope of a border device search (which is presented both here and in *Cano*) turns on the predicate issue of what level of suspicion and process

is required in the first place (which is presented here but not in *Cano*). Thus, the Court should grant certiorari in this case, which presents both inextricably interrelated issues on a developed record. And because the courts of appeals are divided on both the suspicion and scope issues, following the government's suggestion would leave unresolved a conflict among the lower courts on the predicate issue of what suspicion is required.

A. The Fourth Amendment Requires Determining the Standard of Suspicion Before Assessing the Permissible Scope of Search.

The question presented in *Cano* is a limited one: whether the search of an electronic device at the border must be limited in scope to a search for digital contraband. U.S. Br. 7. The government's petition in that case simply *presumes* that warrantless and often suspicionless searches of electronic devices at the border are valid, and takes issue only with the Ninth Circuit's limitation of the search's scope. The Ninth Circuit also operated from that presumption because of circuit precedent on the required level of suspicion for border searches of electronic devices that predates this Court's decision in *Riley v. California*, 573 U.S. 373 (2014). *See Cano*, 934 F.3d at 1007 (citing *United States v. Cotterman,* 709 F.3d 952 (9th Cir. 2013) (en banc)).

But determining whether the Fourth Amendment requires a warrant or individualized suspicion for border searches of electronic devices is a necessary predicate to determining the permissible scope of the search. Indeed, the issue of whether border searches of electronic devices must be limited

in scope only arises *if* such searches may be conducted without a warrant. If a warrant is required, the scope of the search would be determined by the warrant and bounded by the requirement of particularity, rather than by a categorical scope limitation. By contrast, *warrantless* searches "must be limited in scope to that which is justified by the particular purposes served by the [warrant] exception." *Florida v. Royer*, 460 U.S. 491, 500 (1983) (plurality op.); *see also* Pet. Br. 18–19.

Therefore, to decide the scope question presented here and in *Cano*, this Court will *first* need to determine whether border searches of electronic devices require a warrant under the Fourth Amendment.

Moreover, if the Court rejects a warrant requirement, it will still need to determine what level of suspicion is required for such searches, because that issue will necessarily frame its assessment of the search's permissible scope. Even where a warrant is not required, the scope of a search is determined by the suspicion or purpose that justifies the search in the first place. For example, a *Terry* frisk requires reasonable suspicion that the person is armed, and the scope of the search must be limited to a frisk for weapons. *Terry v. Ohio*, 392 U.S. 1, 30–31 (1968).

The ultimate touchstone under the Fourth Amendment is "reasonableness." *Riley*, 573 U.S. at 381 (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)). The reasonableness of a category of searches is determined both by the standard of suspicion required and the search's scope. The appropriate scope of an electronic device search at the border is therefore inextricably intertwined with the

standard of suspicion necessary to justify the search in the first place.

Accordingly, the Court cannot properly decide the scope question without deciding what is required to justify the search in the first place. The Court should grant certiorari in this case because it permits the Court to consider all interrelated aspects of this critical Fourth Amendment question: both the threshold issue of whether a warrant or individualized suspicion is required, and what scope is reasonable.

B. The Courts of Appeals Are Split on Both the Question of What Suspicion Is Required and What Scope Is Permissible.

The government argues that the circuit courts are insufficiently split on the standard of suspicion required for border searches of electronic devices. U.S. Br. 8–9. In fact, the circuit courts are fractured on whether and when such searches require suspicion, and if so, under what standard. *See* Pet. Br. 15–16 (discussing the different rules of the circuit courts requiring, in some cases, no suspicion, reasonable suspicion, or a warrant).

The government seeks to explain away the circuit split on the suspicion standard by contending that the courts of appeals are divided only on what is required for "advanced" searches, not "basic" searches. U.S. Br. 8. But the Fourth Amendment supports no distinction between "basic" and "advanced" searches, both of which can reveal more private information about an individual than the most thorough home searches. *Riley*, 573 U.S. at 396–97. Because that distinction has no foundation in the Fourth Amendment, it cannot explain away the conflict

among the circuits, two of whom require individualized suspicion for border searches, and two of whom do not.

The distinction is an artificial one with no foundation in this Court's Fourth Amendment jurisprudence, and which the government has simply asserted in the policies challenged here. U.S. Br. 2–3. But the fact that the government has chosen to make that distinction does not determine the constitutional analysis. The courts must assess whether the Constitution permits the policies and practices in question. This Court in *Riley* looked at the reasonableness of warrantless electronic device searches as a *category*, without regard to whether they were "basic" or "advanced" as the government calls them. Indeed, the searches in that case were manual (or what the government calls "basic"). *Riley*, 573 U.S. at 379–80, 400.

In a "basic" search, a border officer can read the traveler's emails, text messages, and documents, peruse photos, review contacts, and retrieve browsing history. Pet. App. 214a–17a (¶¶ 64, 67–71, 75). The officer also can use the device's own search tools to efficiently locate content across the device. Pet. App. 216a (¶¶ 70–71). Nothing about a "basic" search requires it to be cursory or limited in time or scope. Pet. App. 293a–94a (§ 5.1.3). There is no reason for this Court to treat "basic" and "advanced" searches as separate categories for Fourth Amendment purposes based on the government's artificial distinction.

Lastly, granting the petition in this case will avoid the need to take up multiple border search cases in successive terms. If this Court were to attempt to address only the question of the permissible scope of

border device searches without assessing what standard of suspicion justifies them in the first place, it would leave the latter question unresolved. But the circuit courts are split on both questions. Pet. Br. 15–16. Resolution of only the scope question presented in *Cano* would not only risk deciding a subsequent question without deciding the prior threshold question, but would provide no guidance to the lower courts on how to resolve their conflict on the standard of suspicion.

By granting this petition, the Court has an opportunity to decide both halves of the full Fourth Amendment question, and to provide much needed guidance to both border officers and the traveling public. Pet. Br. 11–12.

II. THIS CASE PROVIDES AN APPROPRIATE FACTUAL RECORD TO RESOLVE BOTH THE STANDARD OF SUSPICION AND PERMISSIBLE SCOPE OF BORDER DEVICE SEARCHES.

This case presents a robust factual record important to guiding the Court in its resolution of the Fourth Amendment issues presented. The record includes evidence of the substantial privacy interests travelers have in their electronic devices, the weak or nonexistent governmental interests in warrantless border device searches, and the particular privacy harms suffered by Petitioners themselves. And the government's mid-litigation policy changes do not affect the Court's ability to consider the question presented.

A. The Record Affords the Court Valuable Information Upon Which to Assess the Privacy Interests in Electronic Devices and the Governmental Interests in Warrantless Border Device Searches.

Resolution of the question presented here calls for the sort of categorical analysis the Court employed in *Riley* to determine whether the search-incident-to-arrest exception to the Fourth Amendment's warrant requirement applied to cell phones. Like the search-incident-to-arrest exception, the border search exception requires a categorical approach. *See United States v. Ramsey*, 431 U.S. 606, 621 (1977) (noting the similarity between the two warrant exceptions). Contrary to the government's contention, U.S. Br. 10, the record here provides precisely the sort of information upon which such a categorical assessment should rest.

In determining whether to apply the border search exception to a "particular category of effects" such as electronic devices, the Court must consider both individual privacy interests and the government's legitimate interests. *Riley*, 573 U.S. at 385–86. And these interests must be considered as a general matter; otherwise, courts would be required to decide the Fourth Amendment standard anew for every search, based on minor variations in how the search was conducted. The *Riley* Court did not determine its Fourth Amendment rule based on the particular details of the cell phone searches in that case, such as what information law enforcement officers viewed on the phones. Rather, the Court considered the *general* privacy and governmental interests implicated by such searches. *Id.* at 387–91, 393–98 (examining the privacy interests people have

in their cell phones without limiting the analysis to the specific searches at issue, and doing the same for the government's interests).

The thorough factual record in this case specifically addresses the privacy interests that border searches of electronic devices implicate. Pet. App. 214a–21a (¶¶ 63–80). This supplements this Court's detailed analysis of the privacy interests in cell phones, *Riley*, 573 U.S. at 393–98, which is equally applicable to this case.

The record here also includes extensive facts related to the government's asserted purposes in conducting border searches of electronic devices, as well as other facts about the prevalence of digital contraband at the border, and border officers' ability to obtain warrants. Pet. App. 221a–47a (¶¶ 81–119).

All of these facts are important to assessing whether warrantless and suspicionless searches of electronic devices are reasonable, and what scope of such searches is permissible. Pet. Br. 26.

By contrast, the record in *Cano* does not address the privacy and governmental interests implicated by border searches of electronic devices as a categorical matter, and includes information only about the particular searches at issue there.

While it is not necessary in this injunctive suit to assess the specifics of past device searches suffered by Petitioners, as would be required in the context of the exclusionary rule, *see*, *e.g.*, *Davis v. United States*, 564 U.S. 229, 240 (2011), the record here nonetheless includes important details about the searches that illustrate their extraordinary invasiveness. For example, a border officer viewed attorney-client privileged communications on Petitioner Zainab

Merchant's cell phone, Pet. App. 260a (¶ 142); officers expended significant resources to extract three thumb drives of data from Petitioner Matthew Wright's cell phone and camera, Pet. App. 110a (¶ 10); and the government obtained and still retains information from the Petitioners' devices, which Petitioners want expunged, Pet. App. 264a (¶ 150).[1]

The record in this case will accordingly enable the Court to consider the broader context and real-world implications of border searches of electronic devices. In contrast, *Cano* involved post-arrest searches of a single person's device following a border crossing. *Cano*'s facts are not representative of the experiences of the tens of thousands of travelers whose devices are searched at the border each year without a warrant or suspicion, and who are not accused of any wrongdoing. *See* Pet. App. 233a–36a (¶¶ 99–102) (showing a lack of evidence of the effectiveness of warrantless border device searches in uncovering criminal conduct).

B. The Voluntary Changes CBP and ICE Made to Their Policies While This Case Was Pending Do Not Resolve the Question Presented.

Finally, the fact that the government made modest changes to its policies after Petitioners filed this suit does not counsel against review here, because those changes do not affect the question presented. Indeed, the fact that two Petitioners suffered device searches even after filing suit, and after the

[1] These records were filed under seal to preserve the remedy of expungement, which would be mooted by a public filing.

government modified its policies, only underscores the continuing need for review and relief.

When Petitioners filed suit in September 2017, U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) policies permitted suspicionless border searches of electronic devices. Four months later, in January 2018, CBP changed its policy to require "reasonable suspicion of activity in violation of the laws enforced or administered by CBP" for "advanced" searches where there is not a "national security concern." The policy continues to permit "basic" searches without suspicion, however, and imposes no limit on any searches' scope. Pet. App. 195a (¶ 9). ICE changed its policy to require reasonable suspicion for all "advanced" searches but not for "basic" searches, and also imposed no scope limitation. Pet. App. 197a (¶¶ 18–19).

These modifications do not alter, much less resolve, any of the Fourth Amendment questions presented here. Petitioners maintain that border searches of electronic devices, like searches of cell phones incident to arrest, require a warrant—or at a minimum, reasonable suspicion, and any warrantless search must be limited to searching for digital contraband. The policy changes continue to allow highly invasive searches of electronic devices with no warrant, no suspicion, and no limitation on scope.

All Petitioners were subject to intrusive border device searches without a warrant, individualized suspicion, or any limit on the searches' scope. The fact that two Petitioners *also* experienced searches of their devices after filing this case, and after the policies were modified, again without any requirement of a

warrant, individualized suspicion, or any limit on scope, only underscores the continuing need for resolution. And discovery on the relevant governmental interests took place after CBP's and ICE's policy changes. Pet. App. 39a (Dist. Ct. Summ. J. Op.). The record therefore properly reflects the facts necessary for this Court to decide the Fourth Amendment issue.

CONCLUSION

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

Respectfully submitted,

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

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

Esha Bhandari
Counsel of Record
Hugh Handeyside
Nathan Freed Wessler
Ben Wizner
Hina Shamsi
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street,
18th Floor
New York, NY 10004
(212) 549-2500
ebhandari@aclu.org

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

Date: June 4, 2021