No. 20-1505

IN THE

Supreme Court of the United States

ZAINAB MERCHANT, ET AL.,

Petitioners

v.

ALEJANDRO MAYORKAS, SECRETARY OF THE U.S. DEPARTMENT OF HOMELAND SECURITY, in his official capacity, ET AL.

Respondents.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the First Circuit

BRIEF OF *AMICI CURIAE* THE CENTER FOR DEMOCRACY & TECHNOLOGY, THE BRENNAN CENTER FOR JUSTICE, AND TECHFREEDOM IN SUPPORT OF PETITIONER

Trisha Anderson
Counsel of Record
Rafael Reyneri
Andrew Longhi*
COVINGTON & BURLING LLP
850 Tenth Street, NW
Washington, DC 20001
(202) 662-6000
tanderson@cov.com

Counsel for Amici Curiae

TABLE OF CONTENTS

Table of Authorities

Page(s)

Cases

Other Authorities

INTEREST OF *AMICI CURIAE*

Amicus curiae the Center for Democracy & Technology ("CDT") is a non-profit, public interest organization focused on privacy and civil liberties issues affecting the Internet and other digital technologies.[1] CDT represents the public's interest in an open Internet and promotes constitutional and democratic values of free expression, privacy, and non-discrimination in the digital age.

Amicus curiae the Brennan Center for Justice at New York University School of Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice. The Center's Liberty and National Security ("LNS") Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security and law enforcement policies that respect the rule of law and constitutional values. The LNS Program is particularly concerned with domestic surveillance and related law enforcement policies and practices, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on First and Fourth Amendment freedoms.[2]

---

[1] No party or counsel for any party authored any part of this brief or made a monetary contribution intended to fund the preparation or submission of this brief. The parties have consented to the filing of this brief.

[2] This brief does not purport to represent the position, if any, of New York University School of Law.

Amicus curiae TechFreedom is a non-profit, non-partisan think tank dedicated to educating policy-makers, the media, and the public about technology policy. TechFreedom defends the freedoms that make technological progress both possible and beneficial, including the privacy rights protected by the Fourth Amendment, the crown jewel of American civil liberties.

INTRODUCTION AND SUMMARY OF ARGUMENT

Modern travelers crossing the border carry with them electronic devices that contain vast amounts of sensitive information that can reveal every private detail of their lives. Border searches of electronic devices therefore implicate significant privacy interests because, "[w]ith all they contain and all they may reveal," these devices "hold for many Americans 'the privacies of life.'" *Riley v. California*, 573 U.S. 373, 403 (2014) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

The government's policies regarding border searches of electronic devices fail to account for this reality. Each year, border agents perform tens of thousands of invasive searches of electronic devices without procedural safeguards to protect travelers' privacy. These policies attempt to distinguish between basic searches (sometimes called "manual"), for which no individualized suspicion is required, and advanced searches (sometimes called "forensic"), requiring reasonable suspicion unless there is a "national security concern." When performing an advanced search, border agents use external equipment to search the

device. Border agents perform basic searches, which are far more common, on the spot using their hands and eyes. However, the government's distinction between basic and advanced searches is legally immaterial because there is no "meaningful difference between the two classes of searches in terms of the privacy interests implicated." Pet. Ap. 71a-72a. Either kind of search can result in the government's intrusion into the great volume and detail of personal information stored on electronic devices. These policies violate the Fourth Amendment, and this Court's review is needed to provide guidance on this important and recurring question of federal law.

Electronic devices are a vital part of modern life. Many electronic devices combine functions that few contemplated would be performed by one device. These functions reveal information that is increasingly sensitive and private in nature. A quick look at the applications installed on a smartphone, for example, can reveal a user's political associations and activities. A basic search of a device's applications also can reveal sensitive information of other individuals. In addition to the applications installed on electronic devices, the devices themselves can reveal large amounts of data through a basic search, including highly sensitive location history and application usage data. Electronic devices also are used to store passwords. As a result, a basic search of an electronic device can allow a border agent to access the username and password for every online account of that individual, giving them access to highly personal data that the individual intended to keep secure. When all of the information gathered on an electronic

device is considered in the aggregate, the information becomes more than the sum of its parts.

Border searches of electronic devices, whether basic or advanced, can reveal kinds and quantities of information that exceed those underpinning traditional assumptions supporting the border search exception to the Fourth Amendment. Prior to the proliferation of personal electronic devices, the extent to which border searches intruded on the privacy of travelers had been constrained by physical realities—travelers are limited in how many physical effects they can carry. Electronic devices, by contrast, are in practice not subject to comparable constraints due to their ever-increasing storage capacity. Electronic devices also are now ubiquitously used during travel. Whereas before, a border search may have been unlikely to involve a traveler's sensitive belongings, an individual subject to a border search today is likely to be carrying an electronic device that contains "[t]he sum of [the] individual's private life." *Riley*, 573 U.S. at 394. These differences render inapplicable the traditional underpinning for the border search exception. As a result, the border search exception should not be mechanically applied to electronic devices.

Border searches of electronic devices implicate two important issues of federal law: the *scope* of the border search exception, and the *level* of individualized suspicion needed to conduct a border search of an electronic device. The question presented in the petition addresses both issues. By contrast, the petition filed in *United States v. Cano*, No. 20-1043, is narrowly focused on only the first issue without addressing the equally important second aspect.

Moreover, this case is a particularly appropriate vehicle because the question presented calls on the Court to consider the lawfulness of basic searches, which currently require no individualized suspicion at all despite constituting the vast majority of border searches. If the Court is to consider the border search exception, it should not pass on an opportunity to address the aspect of the question that is most impactful to travelers today.

This case also is an appropriate vehicle because it is a civil suit seeking only injunctive relief, unlike the other cases that have addressed the application of the border search exception to electronic devices in the context of criminal cases. The factual record in this case illustrates how the government is increasingly performing border searches of electronic devices without any individualized suspicion, and it reinforces the need for this Court's guidance.

ARGUMENT

I. BORDER SEARCHES OF ELECTRONIC DEVICES INTRUDE ON SIGNIFICANT PRIVACY INTERESTS THAT LIE AT THE CORE OF THE FOURTH AMENDMENT

A. Any Search of an Electronic Device, Whether Basic or Advanced, Can Reveal a Vast Amount of Sensitive Personal Information.

Electronic devices are a vital part of modern life. Eighty five percent of U.S. adults own a smartphone.[3] Eighty five percent of U.S. adults also report that they go online on a daily basis,[4] and thirty one percent report going online "almost constantly."[5] This near universal adoption of electronic devices, along with their constant use, has prompted the Court to recognize their importance in modern life. *See, e.g.*, *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018) (describing a cellphone as "almost a feature of human anatomy"); *see also United States v. Saboonchi*, 990 F. Supp. 2d 536, 557–58 (D. Md. 2014) (referring to electronic devices as "digital umbilical cords to what travelers leave behind at home or at work, indispensable travel accessories in their own

---

[3] *See* Pew Rsch. Ctr., *Mobile Fact Sheet* (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/. Ninety seven percent of U.S. adults own a cellphone of some kind. *Id.*

[4] *See* Pew Rsch. Ctr., *About Three-In-Ten U.S. Adults Say They Are 'Almost Constantly' Online* (Mar. 26, 2021), https://www.pewresearch.org/fact-tank/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/.

[5] *Id.*

right, and safety nets to protect against the risks of traveling abroad").

Many electronic devices combine functions that few contemplated would be performed by one device. These functions reveal information that is increasingly sensitive and private in nature. They contain information that travelers historically would have been unlikely to carry with them: "apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; [and] apps for improving your romantic life." *Riley*, 573 at 396. In other words, the information contained in these devices can reveal an individual's most personal details, including medical and mental health conditions, financial information, sensitive or privileged material about clients, and sexual preferences. A quick look at the applications installed on a smartphone (as is easily possible through a basic search), for example, can reveal a user's political associations and activities, showing at a glance that a traveler is a supporter of a political candidate[6] or that they have been engaged in campaign activities.[7]

---

[6] *See, e.g.*, JoeBiden.com, *Vote Joe Support*, https://joebiden.com/vote-joe-support/ (official Biden campaign app) (last visited May 27, 2021).

[7] NGP VAN, *Canvass with MiniVAN 8*, https://act.ngpvan.com/minivan (describing mobile political canvassing app) (last visited May 27, 2021).

A basic search of a device's applications also can reveal sensitive information of other individuals, including that of minors. For example, because of the ongoing pandemic, many parents have been forced to manage their children's distance learning through their electronic devices. As a result, they must store information about their child's education, including uploaded school assignments, grades, photos, and attendance records, often without a password.[8] Calendar invitations also now contain passwords and one-click connections that could provide access to otherwise highly private conversations should an unintended recipient gain access to an invitation.

In addition to the applications installed on electronic devices, the devices themselves can reveal large amounts of data through a basic search, including highly sensitive location history and application usage data. The iPhone's "Significant Locations" data, for example, is enabled by default and uses geolocation information collected by the device to record locations that the user has visited through precise timestamps as well as the means of transport that brought the user there.[9] This sensitive data is stored on the device, meaning it can be accessed by a basic search.

---

[8] *See e.g.*, Apple, *brightwheel:Child Care App*, https://apps.apple.com/us/app/brightwheel-child-care-app/id902823296 (last visited May 27, 2021) (an early education platform for preschools, child care providers, and daycares that "that integrates everything you need: sign in/out, messaging, learning assessments, daily sheet reports, photos, videos, calendars, scheduling, attendance, online bill pay for parents, and much more.").

[9] Zak Doffman, *Why You Should Stop This 'Hidden' Location Tracking On Your iPhone*, Forbes (Oct 4, 2020),

These devices also generate application tracking data that reveals how frequently an app is used, the exact length of time a user has spent with each app, the number of notifications that a user has received for each app, and even the number of times a person has picked up their phone.[10] This data can allow border agents to focus their searches on applications used most often, which are more likely to contain personal information.

Electronic devices also are used to store passwords.[11] According to a study last year, almost half of Americans adults store sensitive credential data like usernames, passwords, and security or PIN codes on their electronic devices using unsecured note-taking apps.[12] These devices also function as password managers that allow individuals to create and store unique passwords in one place for each of their online

---

https://www.forbes.com/sites/zakdoffman/2020/10/04/apple-iphone-12-location-tracking-in-ios-14-upgrade/; Vladimir Katalov, *Significant Locations, iOS 14 and iCloud*, Elcomsoft Blog (July 9, 2020), https://blog.elcomsoft.com/2020/07/significant-locations-ios-14-and-icloud/.

[10] Apple, *iOS 12 Introduces New Features to Reduce Interruptions and Manage Screen Time* (June 4, 2018), https://www.apple.com/newsroom/2018/06/ios-12-introduces-new-features-to-reduce-interruptions-and-manage-screen-time/.

[11] *See* Apple, *Automatically Fill in Strong Passwords on iPhone*, https://support.apple.com/guide/iphone/automatically-fill-in-strong-passwords-iphf9219d8c9/ios (last visited May 27, 2021).

[12] Spread Privacy, *The Hidden Privacy Risk in Note-Taking Apps* (Feb. 27, 2020), https://spreadprivacy.com/privacy-risks-note-apps/.

accounts.[13] Three of the main mobile browsers (Safari, Chrome, and Firefox) offer built-in password managers, and third-party applications also offer this functionality. These password managers allow users to view any saved password in clear text.[14] As a result, a basic search of an electronic device might conceivably allow a border agent to access the username and password for every online account of that individual, giving them access to highly personal data that the individual intended to keep secure.[15]

Disconnecting an electronic device from the Internet (as the CBP instructs border agents to do) does not

---

[13] *See* Sarah Perez, *Password AutoFill in iOS 12 Will Work with Third-Party Password Managers*, Tech Crunch (June 5, 2018), https://techcrunch.com/2018/06/05/password-autofill-in-ios-12-will-work-with-third-party-password-managers/.

[14] In some circumstances, such as with the iPhone's password manager, this may require the user to re-enter the password used to unlock the device itself or to use biometrics, such as a face scan, to access the stored passwords. *See* Dave Johnson, *How to Find All of Your Saved Passwords on an iPhone, and Edit or Delete Them*, Business Insider (Aug. 28, 2019), https://www.businessinsider.com/how-to-find-passwords-on-iphone.

[15] CBP's policy states that "[p]asscodes and other means of access obtained during the course of a border inspection . . . will be deleted or destroyed when no longer needed to facilitate the search of a given device." Pet. Ap. at 298a. However, CBP's Privacy Impact Assessment limits this restriction to "passcodes or other means of access *provided by the traveler*." CBP, Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices at 9, 19 (Jan. 4, 2018) (emphasis added). This raises a question whether CBP may keep passwords they find in a device that the traveler did not affirmatively provide, or that do not relate to unlocking the device itself. Furthermore, CBP asserts that "information may be detained or retained from a traveler's electronic device for a wide variety of purposes." *Id*.

fully mitigate the severity of the intrusion of a basic search. Due to "caching," a process that generally occurs without a user's awareness, electronic devices store reams of downloaded personal information directly on the device rather than (or in addition to) using cloud-based storage. "Caching is the process of saving data temporarily so the site, browser or app doesn't need to download it each time."[16] As a result of caching, anything from a user's music history to their most confidential information can be found in the device itself, without a need to connect to the Internet—*i.e.*, through a basic search.

Cloud-based services market this as a feature that enables people to access their files, social media accounts, inboxes, and videos on the go. Without connecting to the Internet, for example, users can work in a Google Document, browse and draft posts to Facebook, read email, or watch a movie through their streaming subscription.[17] Similarly, Gmail can be accessed even when a device has been disconnected from

---

[16] Lee Bell, *What Is Caching and How Does It Work?*, Wired (May 7, 2017), https://www.wired.co.uk/article/caching-cached-data-explained-delete.

[17] Google, *Work on Google Docs, Sheets, & Slides Offline,* https://support.google.com/docs/answer/6388102 (last visited May 27, 2021); Sarah Perez, *Facebook Gets an Offline Mode*, Tech Crunch (Dec. 10, 2015), https://techcrunch.com/2015/12/10/facebook-gets-an-offline-mode/; Microsoft, *Using Outlook Web App Offline*, https://support.microsoft.com/en-us/office/using-outlook-web-app-offline-3214839c-0604-4162-8a97-6856b4c27b36 (last visited May 27, 2021); Amazon, *Download Prime Video Titles*, https://www.amazon.com/gp/help/customer/display.html/ref=vnid_GTDVUQFMY3GTZVX7?nodeId=GTDVUQFMY3GTZVX7 (last visited May 27, 2021).

the Internet.[18] This cached data can amount to gigabytes' worth of information stored directly on the device.

Users are not likely to be aware of what particular information has been cached. Many apps and websites cache data using background processes that are not discernible to the user, meaning that an user's device may download data without her awareness.[19] It can be difficult for individuals to navigate the various technical settings to determine the ways in which a given app caches or stores their data.[20] As a result, data that a user believed was stored only in the cloud may in fact be present locally on the device—and accessible through a basic search. In these circumstances, it often is unclear where a device's hardware ends and where the "cloud" begins.[21]

---

[18] Google, *Use Gmail Offline*, https://support.google.com/mail/answer/1306849 (last visited May 27, 2021).

[19] *See* Bell, *supra*, note 16.

[20] *See* Olivia Young, *How to Clear the Cache on Your iPhone to Free up Storage Space and Help It Run Faster*, Business Insider (Feb. 13, 2019), https://www.businessinsider.in/how-to-clear-the-cache-on-your-iphone-and-make-it-run-faster/articleshow/67967842.cms; Michelle Greenlee, *How to Clear the Cache on Your Android Phone to Make It Run Faster*, Business Insider (Mar. 21, 2019), https://www.businessinsider.com/how-to-clear-cache-on-android-phone.

[21] Some users seek to protect their online privacy by disabling cloud storage, so that their information can be found only on the device itself. But disabling cloud storage does not shield the information stored on the device from a manual search.

In any event, it appears that border agents are not regularly disconnecting electronic devices from the Internet when performing border searches, compounding the privacy invasion. A review by the Inspector General of the Department of Homeland Security regarding Customs and Border Protection's ("CBP") compliance with its border search policies between April 2016 and July 2017 found that, contrary to the agency's stated policies, "officers did not consistently disconnect electronic devices, specifically cellphones, from the network before searching them."[22] Moreover, CBP's method of disconnecting a device from the Internet—asking the user to place it in airplane mode[23]—does not ensure that the device will in fact not be able to connect to the Internet. Devices that are placed on airplane mode often maintain their connection to known Wi-Fi networks,[24] like the kind commonly available to the public in U.S. airports. This connection can allow an agent to access data stored in the cloud. In these instances, the line between the device and the cloud disappears, and the

---

[22] Office of Inspector General, *CBP's Searches of Electronic Devices at Ports of Entry - Redacted,* OIG-19-10 (Dec. 3, 2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-12/OIG-19-10-Nov18.pdf. Although the period reviewed in the report predates the policies at issue in this case, there is no evidence in the record the government has resolved these failings.

[23] U.S. Customs and Border Protection, *Border Search of Electronic Devices*, CBP Directive No. 3340-049A § 5.1.2 (Jan. 4, 2018), https://www.dhs.gov/sites/default/files/publications/CBP%20Directive%203340-049A_Border-Search-of-Electronic-Media.pdf.

[24] Michael Potuck, *How to Use Wi-Fi With Airplane Mode on iPhone*, 9 to 5 Mac (Oct. 12, 2018), https://9to5mac.com/2018/10/12/wi-fi-airplane-mode-iphone/.

search is no longer one of an electronic device at the border. Rather, the search is capable of reaching the entire universe of an individual's private information even though that information is stored on a server located within the territorial jurisdiction and has not and will not cross the border.[25] *See Riley*, 573 U.S. at 397 (noting that "Internet-connected devices [] display data stored on remote servers rather than on the device itself").

When all of the information gathered on an electronic device is considered in the aggregate, the information becomes more than the sum of its parts. A basic search of an electronic device can reveal information that reconstructs the owner's entire life—both professional and private—in intimate detail extending back weeks, years, or even decades. *See Riley*, 573 U.S. at 394 (cellphones enable "[t]he sum of an individual's private life [to] be reconstructed through a thousand photographs labeled with dates, locations, and descriptions"). By searching a traveler's electronic device, even without resorting to the external tools that define an advanced search, a border agent can recreate essentially every detail of the traveler's life and history, leveraging geo-location information, phone use information, cached application data, user accounts, and passwords. Such a detailed and extensive search, whether basic or advanced, can reveal kinds and quantities of information that exceed those

---

[25] *See* Quentin Hardy, *Ask the Times: 'Where Does Cloud Storage Really Reside? And Is It Secure?'*, N.Y. Times (Jan. 23, 2017), https://www.nytimes.com/2017/01/23/insider/where-does-cloud-storage-really-reside-and-is-it-secure.html (electronic devices make use of "cloud computing systems . . . that span the globe").

underpinning traditional assumptions supporting the border search exception to the Fourth Amendment.

B. Traditional Assumptions Grounding the Border Search Exception Do Not Apply to Electronic Devices Because of the Vast Quantities of Information These Devices Contain.

Prior to the proliferation of personal electronic devices, the extent to which border searches intruded on the privacy of travelers had been constrained by physical realities. Put simply, travelers are limited in how many physical effects they can carry. *Cf. Riley*, 573 U.S. at 375 ("Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.").

Electronic devices, by contrast, are in practice not subject to comparable constraints due to their ever-increasing storage capacity. The extent to which border searches of such devices intrude on the privacy of travelers is equally unconstrained. For example, in *Riley*, the Court noted that the top-selling smartphone at the time had "a standard capacity of 16 gigabytes," which "translate[d] to millions of pages of text, thousands of pictures, or hundreds of videos." *Id.* at 394. The minimum storage of the latest version of that same smartphone is now 64 gigabytes, and a user can choose a version of the phone with storage up to 512

gigabytes.[26] Other popular smartphones can triple that storage capacity to 1.5 terabytes using microSD cards.[27] Crossing the border with a device that holds 1.5 terabytes of information, for example, is the physical equivalent of traveling with approximately 1,950 physical filing cabinets of paper.[28]

The storage capacity of electronic devices continues to increase. There are smartphones on the market today that can support a 2 terabyte microSD card,[29] and laptops (including those designed to be used while on the go) commonly contain that much internal storage capacity.[30] Some tablets can support a full-size SD card,[31] meaning they soon could hold 128 terabytes of

---

[26] Apple, *Apple 12 Pro*, https://www.apple.com/shop/buy-iphone/iphone-12-pro (last visited May 27, 2021).

[27] *See* Samsung, *Android Galaxy S20 5G: Specifications*, https://www.samsung.com/us/mobile/galaxy-s20-5g/specs/ (last visited May 27, 2021).

[28] *See* Dropbox, *How Much Is 1 TB of Storage?* (determining that one terabyte of data is equivalent to "6.5 million document pages" or "1,300 physical filing cabinets"), https://www.dropbox.com/features/cloud-storage/how-much-is-1tb (last visited May 27, 2021).

[29] LG, *Tech specs: LG G8 ThinQ*, https://www.t-mobile.com/support/devices/android/lg-g8-thinq/tech-specs-lg-g8-thinq (last visited May 27, 2021).

[30] *See, e.g.*, Apple, *MacBook Air*, https://www.apple.com/macbook-air/specs/ (last visited May 27, 2021).

[31] Microsoft, *Surface Book 3 for Business*, https://www.microsoft.com/en-us/surface/business/surface-book-3 (last visited May 27, 2021).

storage.[32] That is more than six times the amount of text stored in the entire Library of Congress.[33] These examples illustrate that the amount of information that can be contained in such massive storage devices dwarfs what travelers historically could bring in their luggage or vehicles.

Electronic devices also are now ubiquitously used during travel. For example, one survey found that over 70% of U.S. travelers report that they "always" travel with their smartphone—a figure that was increased from 41% in 2015.[34] Americans use their electronic devices to communicate with family and friends while abroad, and store travel documents, such as boarding passes. Whereas historically a border search may have been unlikely to involve a traveler's sensitive belongings, an individual subject to a border search today is likely to be carrying an electronic device that contains "[t]he sum of [the] individual's private life." *Riley*, 573 U.S. at 394.

This revolutionary change in the quantity and nature of data exposed through border searches of electronic devices relative to searches of physical containers like luggage renders inapplicable the

---

[32] Dani Deahl, *SD Cards Could Soon Hold 128TB of Storage*, The Verge (Jun. 28, 2018), https://www.theverge.com/2018/6/28/17514660/sd-card-128tb-storage.

[33] *See* Guinness World Records, Guinness World Records 2017205 (2016) ("[T]he text content of the entire Library of Congress is equivalent to 20 TB.").

[34] Google, *How Smartphones Influence the Entire Travel Journey in the U.S. and Abroad* (Feb. 2018), https://www.thinkwithgoogle.com/consumer-insights/consumer-journey/consumer-travel-smartphone-usage/.

traditional underpinning for the border search exception, premised on travelers carrying physical containers with limited storage capacity. *Cf. Carpenter*, 138 S. Ct. at 2214 (recognizing "'immense storage capacity' of modern cell phones in holding that police officers must generally obtain a warrant before searching the contents of a phone" (quoting *Riley*, 573 U.S. at 393)). The Court therefore must revisit the Fourth Amendment underpinnings of the border search exception as applied to electronic devices.

II. THE DECISION BELOW IS AN IDEAL VEHICLE TO RESOLVE A RECURRING QUESTION OF NATIONAL IMPORTANCE.

A. The Question Presented in the Petition Addresses Both Aspects of This Important and Recurring Issue.

Border searches of electronic devices implicate two important issues of federal law. First, the *scope* of the border search exception *vis-à-vis* digital devices—*i.e.*, is the exception limited to searches for digital contraband? Second, the *level* of individualized suspicion needed to conduct a border search of an electronic device—whether a warrant based on probable cause is required, or whether the officer must have at least reasonable suspicion. The question presented in the petition addresses both issues. And for the reasons noted in the petition, the Court's guidance is needed with respect to both issues.

The petition filed in *United States v. Cano*, No. 20-1043, by contrast, is narrowly focused on only the first

issue (scope) but does not address the equally important second aspect (level of suspicion needed). If the Court were to address only the scope of the border exception, travelers and border agents would be left without an understanding of when a border search of an electronic device is appropriate or lawful.

This case is a particularly appropriate vehicle because the question presented calls on the Court to consider the lawfulness of basic searches that currently require no individualized suspicion at all. Basic searches constitute the vast majority of border searches. *See* Pet. Ap. 207a–209a. And as explained above, basic searches can be as intrusive as advanced ones. As a result, basic searches, *in the aggregate*, represent the greater privacy intrusion, and the question of their lawfulness is just as important as—if not more important than—the scope of the border exception. If the Court is to consider the border search exception, it should not pass on an opportunity to address the aspect of the question that is most impactful to travelers today.

B. The Decision Was Premised on a Developed Factual Record That Highlights the Full Extent of the Privacy Interests at Stake.

This case also is an appropriate vehicle because it is a civil suit seeking only injunctive relief in which Petitioners have established that they have been and will continue to be repeatedly subjected to the government's unconstitutional policies. As a result, there is a fully developed factual record that can assist this Court's review. This is unlike the other cases that

have addressed the application of the border search exception to electronic devices in the context of criminal cases, which typically have involved only a single search.

The factual record in this case demonstrates why this question is of national importance and how the government's border search policies intrude on the privacy of innocent Americans without justification. Petitioners include people from all walks of life. Pet. Ap. 2–3. None has been accused of a crime. *See id.* at 2–5. Nevertheless, all petitioners had their electronic devices searched with no explanation given. *See id.* Three petitioners had their devices searched multiple times, including *after* filing the instant action. *Id.* at 5. At least four had their personal information retained by government agents. *Id.* One petitioner had his devices taken from him for months. *Id.* at 4–5. The kind of information that was searched was sensitive in nature, including legally confidential materials. *Id.* at 3. And the searches intruded on the religious rights of at least one petitioner, whose personal pictures were viewed by a male agent, in contravention of her religious beliefs. *Id.* at 3. Finally, although some of these searches used external equipment, *id.* at 4, the record shows that most were basic searches that involved no such equipment.

Thus, this case presents a well-developed record across a variety of fact patterns that will inform the Court's consideration of the legal issues. This record illustrates how the government is increasingly performing border searches of voluminous private information accessible through electronic devices without any individualized suspicion, resulting in a

serious invasion of privacy. And it reinforces the need for this Court's guidance as to both of the issues in the question presented in the petition.

CONCLUSION

For the foregoing reasons the petition should be granted.

Respectfully submitted,

Trisha Anderson
Counsel of Record
Rafael Reyneri
Andrew Longhi*
COVINGTON & BURLING LLP
850 Tenth Street, NW
Washington, DC 20001
tanderson@cov.com
(202) 662-6000

May 2021

Counsel for Amici Curiae

*Admitted to the Bar under DC App. R. 46-A (Emergency Examination Waiver); Practice Supervised by DC Bar members.