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, NO. 1:17-CV-11730 (CASPER, J.)

CORRECTED BRIEF OF THE CENTER FOR DEMOCRACY & TECHNOLOGY, THE BRENNAN CENTER FOR JUSTICE, R STREET INSTITUTE, AND TECHFREEDOM AS *AMICI CURIAE* IN SUPPORT OF PLAINTIFFS-APPELLEES/CROSS-APPELLANTS AND AFFIRMANCE IN PART AND REVERSAL IN PART

Kurt Wimmer
Rafael Reyneri
Calvin Cohen
Frank Broomell
COVINGTON & BURLING LLP
850 Tenth Street, NW
Washington, DC 20001
(202) 662-6000
rreyneri@cov.com

Counsel for Amici Curiae

August 17, 2020

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amici curiae* make the following disclosures:

Amicus curiae the Center for Democracy and Technology states that it has no parent corporation and that, because it is a non-stock corporation, no publicly held corporation owns 10% or more of its stock.

Amicus curiae the Brennan Center for Justice states that because it is a non-stock corporation, it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

Amicus curiae R Street Institute is a not-for-profit corporation incorporated under the laws of Washington D.C. It has no shareholders, parents, subsidiaries or affiliates.

Amicus curiae TechFreedom is a not-for-profit, non-stock corporation organized under the laws of the District of Columbia with federal tax-exempt 501(c)(3) status. TechFreedom has no parent corporation. It issues no stock.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

STATEMENT OF INTEREST

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, other communications networks, and associated technologies.[1] CDT represents the public's interest in an open Internet and promotes constitutional and democratic values of free expression, privacy, and individual liberty 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

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(2), *amici* certify that all parties have consented to the filing of this brief. No party's counsel authored this brief in whole or in part, no party or party's counsel contributed money that was intended to fund the preparation or submission of this brief, and no person—other than *amici*, its members, or its counsel—contributed money that was intended to fund the preparation or submission of this brief.

personal data, and the concomitant effects on First and Fourth Amendment freedoms.[2]

Amicus curiae R Street Institute (R Street) is a non-profit, non-partisan public-policy research organization. R Street's mission is to engage in policy research and educational outreach that promotes free markets, as well as limited yet effective government, including properly calibrated legal and regulatory frameworks that support national security while safeguarding privacy and individual liberty.

Amicus curiae TechFreedom is a non-profit, non-partisan think tank dedicated to educating policymakers, 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 digital devices that contain vast amounts of sensitive information. Searches of these devices can reveal every private detail of an individual's life. Yet border agents perform invasive searches of digital devices without procedural safeguards to protect travelers' privacy. The Fourth Amendment prohibits such warrantless searches.

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

Border searches of digital devices 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)). For devices like smartphones, this information is available at the touch of a finger.

The Government's policies regarding border searches of digital devices fail to account for this reality even as border agents conduct tens of thousands of searches each year. These policies attempt to distinguish between manual (sometimes called "basic") searches and forensic (sometimes called "advanced") searches. Addendum 5. When performing a forensic search, border agents use external equipment to search the device, whereas border agents perform manual searches on the spot using their hands and eyes. The Government contends that manual searches do not require any individualized suspicion, while forensic searches require reasonable suspicion. But the Government's distinction between manual and forensic searches is untenable because there is no "meaningful difference between the two classes of searches in terms of the privacy interests implicated." Addendum 34.

In determining whether to apply the border search exception to searches of digital devices, this Court must balance the privacy interests of individuals against the government's interest. *See Riley*, 573 U.S. at 385. In this context, the privacy interests at stake lie at the core of the Fourth Amendment, while the Government's

interests are attenuated because most digital devices are unlikely to contain contraband, the identification of which serves as the historical basis for the border search exception. As a result, this Court should hold that a warrant is required to perform manual and forensic border searches of digital devices. Alternatively, this Court should affirm that border searches, manual and forensic, require at least reasonable suspicion the device searched contains digital contraband.

ARGUMENT

I. Digital Devices Subject to Border Searches Contain Vast Quantities of Sensitive Information, Undermining the Justification for the Border Search Exception.

A. A Manual Search of a Digital Device can Reveal a Vast Amount of Sensitive Personal Information.

Digital devices are a vital part of modern life. Eighty one percent of U.S. adults own a smartphone.[3] On average, cellphone users look at their devices 47 times per day,[4] and for younger adults, that number increases to 86 times per day.[5] This near universal adoption of digital devices, along with their constant use, has led courts to emphasize 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

[3] *See* Pew Research Ctr., *Mobile Fact Sheet* (Jun. 12, 2019), https://perma.cc/Y83H-SQUA. Ninety six percent of U.S. adults own a cellphone of some kind. *Id.*

[4] Deloitte, *Americans Look at Their Smartphones More Than 12 Billion Times Daily, Even as Usage Habits Mature and Device Growth Plateaus* (Nov. 15, 2017), https://perma.cc/8HUQ-LMUH.

[5] *Id.*

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

Many digital 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 U.S. at 396. In other words, the information contained in these devices can reveal an individual's most private details, including infirmities and medical conditions, financial information, romantic interests and sexual preferences. A quick look at the applications installed on a smartphone, for example, can reveal a user's political associations and activities, betraying the fact that a traveler is a supporter of a political candidate[6] or that they

[6] *See, e.g.*, Biden for President, *Team Joe Campaign App*, https://perma.cc/27W7-QBAB (official Biden campaign app); Donald J. Trump for President, *Official Trump 2020 App*, https://perma.cc/U34G-L5MW (official Trump campaign app).

have been engaged in campaign activities.[7] A search through a device's applications also may reveal other individuals' sensitive information, 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 digital devices—and as a result must store their children's education records on their devices.[8]

In addition to the applications installed on digital devices, the devices themselves can reveal large amounts of sensitive data, such as location history and application usage, to any user of the device. The iPhone's "Significant Locations" data, for example, uses geolocation information collected by the device to record locations that the user has visited and when the user visited each location—all accessible with just a few taps on the screen.[9] Application tracking data 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 allows a border

[7] NGP VAN, *Canvass with MiniVan 8*, https://perma.cc/QLV8-WBSR (describing mobile political canvassing app).

[8] *See, e.g.*, Seesaw, *Remote Learning with Seesaw*, https://perma.cc/L5PY-VJXH.

[9] Vladimir Katalov, *Apple Probably Knows What You Did Last Summer*, Elcomsoft Blog (Jun. 5, 2018), https://perma.cc/2D3D-NL5H; Dwight Silverman, *Your smartphone knows where you've been, puts it on a map*, Houston Chronicle (Oct. 11, 2017), https://perma.cc/TZS8-F7DC.

[10] *See* Apple, *iOS 12 Introduces New Features to Reduce Interruptions and Manage Screen Time* (June 4, 2018), https://perma.cc/NY2A-WFJA.

agent to easily identify where a user lives and works, and focus their manual search on applications that are frequently used to store or communicate private information or data.

Digital devices also are used as password managers.[11] Password managers allow individuals to create and store strong, unique passwords in one place for each of their online accounts.[12] Three of the main mobile browsers (Safari, Chrome, and Firefox) offer built-in password managers, and third-party apps also offer this functionality. These password managers permit users to read any saved password in clear text.[13] As a result, a search of a digital device may allow a border agent to access the username and password for every online account of that individual.[14]

---

[11] Sarah Perez, *Password AutoFill in iOS 12 Will Work with Third-Party Password Managers*, Tech Crunch (June 5, 2018), https://perma.cc/AH4C-UMQ2.

[12] *Id.*

[13] 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. Dave Johnson, *How to Find All of Your Saved Passwords on an iPhone, and Edit or Delete Them*, Business Insider (Aug. 28, 2019), https://perma.cc/P2F2-7PRL.

[14] 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." CBP Directive 3340-049A ¶ 5.3.2. 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 suggests that CBP may keep passwords they find in a device that the traveler did not affirmatively provide, or that do not relate to unlocking the

Disconnecting a digital device from the Internet at most only partially mitigates the severity of the intrusion of a manual search because, using a process called "caching," digital 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."[15] It is similar to how a person's brain can recognize landmarks after they first visit a location, allowing them to arrive there faster next 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.

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 phone has been

---

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.*

[15] Lee Bell, *What Is Caching and How Does It Work?*, Wired (May 7, 2017), https://perma.cc/V2TA-R69S.

[16] *Id.*

[17] *See* Melanie Pinola, *Make Google Docs, Spreadsheets, and Presentations Work Offline*, IT World (Apr. 26, 2013), https://perma.cc/44DQ-8LSB; Sarah Perez,

disconnected from the Internet.[18] This cached data can amount to gigabytes' worth of information stored directly on the device. Many apps and websites cache data using background processes that are not visible to most individuals, meaning that an individual'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, it often is unclear where a device's hardware ends and where the "cloud" begins.[21]

In any event, it appears that border agents are not regularly disconnecting digital devices from the Internet when performing border searches, compounding the private invasion. A review by the Inspector General of the Department of Homeland Security regarding Customs and Border Protection's ("CBP")

Facebook Gets an Offline Mode, Tech Crunch (Dec. 10, 2015), https://perma.cc/Q5K5-3HKQ; Microsoft, *Using Outlook Web App Offline*, https://perma.cc/PLG8-MJFG; Amazon, *Download Prime Video Titles*, https://perma.cc/386J-WFUJ.

[18] Google, *Use Gmail Offline*, https://perma.cc/ZYR8-AQG7.

[19] *See* Bell, *supra*, note 15.

[20] *See* Olivia Young, *How to Clear the Cache on Your iPhone to Free up Storage Space and Help It Run Faster*, Business Insider (Jun. 27, 2019), https://perma.cc/M56Z-2PWG; Michelle Greenlee, *How to Clear the Cache on Your Android Phone to Make It Run Faster*, Business Insider (Mar. 21, 2019), https://perma.cc/UC8X-ABTQ.

[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.

compliance with its border search policies between 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] In these instances, the line between the device and the cloud disappears, and the search is no longer one of a digital device at the border. Rather, the search becomes capable of reaching the entire universe of an individual's private information even if that information has been stored on a server that in all likelihood is located far from the border.[23] *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 a digital device is considered in the aggregate, the information becomes more than the sum of its parts: a digital 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

[22] Office of Inspector General, *CBP's Searches of Electronic Devices at Ports of Entry* (Dec. 3, 2018), https://perma.cc/Q7BR-ZR6C. 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] *See* Quentin Hardy, *Ask the Times: 'Where Does Cloud Storage Really Reside? And Is It Secure?'*, N.Y. Times (Jan. 23, 2017), https://perma.cc/UF3B-8VLS (digital devices make use of "cloud computing systems … that span the globe").

[to] be reconstructed through a thousand photographs labeled with dates, locations, and descriptions"). By searching a traveler's digital device, a border agent may be able to recreate every detail of the traveler's life and history by leveraging geolocation information, phone use information, cached application data, user accounts, and passwords. Such a detailed and extensive search, whether manual or forensic, can reveal kinds and quantities of information that exceed the traditional assumptions supporting the border search exception to the Fourth Amendment.

B. The Vast Quantities of Information That Digital Devices Contain Exceed What Travelers Have Traditionally Carried When Crossing the Border.

Historically, the extent to which border searches intrude on the privacy of travelers has been subject to physical constraints, as travelers are limited in how many physical effects they can carry. But due to their ever-increasing storage capacity and ability to cache information from the Internet, searches of digital devices are essentially unbounded by physical constraints. For example, in *Riley*, the Supreme 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." *Riley*, 573 U.S. at 394; *see also United States v. Wurie*, 728 F.3d 1, 8 (1st Cir. 2013). The current version of that same smartphone

has a minimum storage of 64 gigabytes, which can be increased to 512 gigabytes.[24] Some devices can triple that storage capacity to 1.5 terabytes using microSD cards.[25] 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. This trend is increasing. Some smartphones already can support a 2 terabyte microSD card,[26] and some tablets can support a full-size SD card,[27] meaning they soon could hold 128 terabytes of storage.[28] That is more than six times the amount of text stored in the entire Library of Congress.[29] That makes a border search of a digital device categorically different from a search of a traveler's luggage.

The scope of the data in such massive storage devices dwarfs what travelers historically could bring in their luggage or vehicles. This exponential difference in the data and information that searches of digital devices implicate means that the traditional justification for the border search exception, premised on travelers

[24] *See* Apple, *The Apple iPhone 11 Pro*, https://perma.cc/G6TM-4LV8.

[25] *See* Samsung, *Android Galaxy S20 5G: Specifications*, https://perma.cc/84Q6-K6WL.

[26] LG, *LG G8 ThinQ: Technical Specifications*, https://perma.cc/5GXF-4J6A.

[27] Microsoft, *Surface Book 3*, https://perma.cc/A84A-6JMU.

[28] 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.

[29] *See Guinness World Records 2017*, at 205 (2016) ("[T]he text content of the entire Library of Congress is equivalent to 20 TB.").

carrying physical containers with limited storage capacity like luggage, is inapplicable. *See Carpenter*, 138 S. Ct. at 2214 (recognizing "'immense storage capacity' of modern cellphones in holding that police officers must generally obtain a warrant before searching the contents of a phone" (quoting *Riley*, 573 U.S. at 393).

II. The District Court Erred in Holding that the Fourth Amendment's Warrant Requirement Does Not Apply to Border Searches of Digital Devices.

The District Court correctly reasoned that both manual and forensic searches require some form of particularized suspicion because there is no "meaningful difference between the two classes of searches in terms of the privacy interests implicated." Addendum 33. However, the District Court erred in finding that reasonable suspicion is sufficient for border searches of digital devices. *Id.* The Fourth Amendment requires a warrant unless certain narrow exceptions apply, including the border search exception. The Supreme Court's decision in *Riley* demonstrates that, in deciding whether to apply a warrant exception in a novel technological context, courts apply traditional Fourth Amendment principles, balancing the privacy interests at stake against the government's interest. *Riley*, 573 U.S. at 385. Searches of digital devices intrude extensively into individuals' privacy, and the government's traditional justification for the border search exception—the need to intercept contraband—is far less relevant here in light of the non-physical nature of the information these devices carry. Therefore, this Court should follow

the Supreme Court's reasoning in *Riley* and require a warrant for border searches of digital devices.

A. The Fourth Amendment Requires Courts to Determine Whether the Border Search Exception Applies by Balancing an Individual's Privacy Interests Against the Government's Interest.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. A warrant generally is required to protect the Fourth Amendment's "ultimate touchstone": reasonableness. *Riley*, 573 U.S. at 382. "When an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable," the Supreme Court has "held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Carpenter*, 138 S. Ct. at 2213.

Over time, courts have recognized narrow exceptions to the Fourth Amendment's general warrant requirement. Searches falling within the scope of these exceptions are reasonable, despite the absence of warrant, due to the government's heightened interest or an individual's lowered privacy expectations.

These exceptions are not absolute and require reevaluation in light of new technologies. *Carpenter*, 138 S. Ct. at 2222 ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents."). The application of the Fourth Amendment in novel factual

contexts can raise heightened privacy concerns, *see id.* at 2214, and these expanded privacy concerns can undermine the basis for an exception to the warrant requirement, *see Riley*, 573 U.S. at 386-87. Where "'privacy-related concerns are weighty enough' a 'search may require a warrant, notwithstanding the diminished expectations of privacy'" that originally justified the exception. *Id.* at 392 (quoting *Maryland v. King*, 569 U.S. 435, 463 (2013)).

In *Riley*, the Supreme Court narrowed one such exception—for searches incident to arrest—holding that the exception does not apply to searches of cellphones because such devices hold the very "privacies of life" that the Fourth Amendment was meant to protect. *Id.* at 403. *Riley* reaffirms that courts must determine whether a warrant exception applies in a novel technological context by applying a traditional Fourth Amendment analysis: "by assessing, on the one hand, the degree to which [the search at issue] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Id.* at 385-86.

This Court should follow *Riley*'s reasoning and apply established Fourth Amendment principles to find that the border exception does not apply to searches of digital devices. The traditional warrant requirement should apply because the privacy interests at stake outweigh the government's interest.

B. Searches of Digital Devices Implicate Significant Privacy Interests That Lie at the Core of the Fourth Amendment.

The border search exception, like the doctrine regarding searches incident to arrest, was developed in the context of physical searches limited by physical constraints. Travelers can carry with them only so much luggage, and what they do carry (*e.g.*, clothes and toiletries) typically does not reveal sensitive information. A search of these effects represents a limited intrusion on privacy. *See 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.").

A border search of a digital device, however, can intrude into an individual's privacy far more than the search of a traveler's physical belongings. As discussed above, a search of a digital device is not akin to a traditional border search of physical property. To assert otherwise "is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." *Riley*, 573 U.S. at 393. The border search exception should not apply to digital devices as these devices are different in character from the "physical realities" of items such as luggage and vehicles that traditionally have constrained the exception's reach. *See Kyllo v. United States*, 533 U.S. 27, 37 (2001) ("[T]he rule we adopt must take account of more sophisticated systems that are already in use or in development.").

Courts increasingly have acknowledged that searches of digital devices raise

heightened privacy concerns because of the immense amounts of personal information that can be gleaned from such devices. The Supreme Court's recent Fourth Amendment jurisprudence reflects this evolution, demonstrating a growing concern regarding the unbound potential for surveillance resulting from digital technologies.

In 2012, the Supreme Court held that the use of a GPS device to monitor an individual's movements can constitute a search requiring a warrant. *United States v. Jones*, 565 U.S. 400, 404 (2012). Though the Court split in its reasoning, it was motivated in part by how technologically-enabled surveillance could enable previously unfeasible privacy invasions. *See id.* at 430 (Alito, J., concurring) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

In 2014, the Supreme Court limited the warrant exception for searches incident to arrest, holding that the exception does not apply to searches of cellphones. *Riley*, 573 U.S. at 403. The Court again reflected the privacy interests implicated by searches of digital devices, reasoning that such searches enable "[t]he sum of an individual's private life [to] be reconstructed through a thousand photographs labeled with dates, locations, and descriptions." *Id.* at 395.

And in 2018, the Supreme Court narrowed the third-party doctrine, holding

that searches of historical cell-site location information, at least for any appreciable period of time, require a warrant. *Carpenter*, 138 S. Ct. at 2221. The Court recognized that a cellphone is "almost a feature of human anatomy, track[ing] nearly exactly the movements of its owner." *Id.* at 2218 (citation and internal quotation marks omitted); *see also id.* ("A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.").

Appellate courts similarly have acknowledged the privacy implications of searches of digital devices. For example, the Fourth Circuit has recognized that "[s]martphones and laptops contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails, and also may provide access to data stored remotely." *United States v. Kolsuz*, 890 F.3d 133, 145 (4th Cir. 2018) (citations omitted). This kind of intimate information "generates 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." *Id*. (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). Moreover, digital devices are "ubiquitous" and necessary for travel. *Id.* This makes the privacy intrusion of a digital device search unlike that of "a routine luggage search," which a traveler can mitigate "by leaving behind her … especially personal effects." *Id.*; *see also United States v. Cano*, 934 F.3d 1002, 1020

(9th Cir. 2019) ("[A] search of a cell phone may give the government not only 'sensitive records previously found in the home,' but 'a broad array of private information never found in a home in any form—unless the phone is.'" (quoting *Riley*, 573 U.S. at 393-97)).

Finally, the government's increasing use of border searches of digital devices underscores the growing privacy interests at stake. CBP has reported that in fiscal year 2019, it "conducted 40,913 border searches of electronic devices"—up from 33,296 in fiscal year 2018 and 30,200 in fiscal year 2017.[30] And these figures may be underinclusive, given that CBP agents do not document every device search. App. 296-98. Similarly, Immigration and Customs Enforcement, which also searches digital devices at the border, fails to maintain records on the number of manual searches it conducts. App. 295-96. The government's increasing reliance on border searches of digital devices reinforces the scope and impact of the Fourth Amendment intrusion at issue.

C. The Government's Interests in Border Searches of Digital Devices Are Attenuated.

The border exception to the warrant requirement is premised on the "long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country." *United States v. Ramsey*, 431 U.S. 606, 616

[30] CBP, *CBP Statement on Border Search of Electronic Devices* (Oct. 30, 2019), https://perma.cc/W2CL-JCJV.

(1977). The exception is intended to advance the government's interest in immigration and customs enforcement by "requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in." *Carroll v. United States*, 267 U.S. 132, 154 (1925); *see also United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985) (border exception premised on government's authority "to regulate the collection of duties and to prevent the introduction of contraband into this country").

Border searches of digital devices cannot be justified on the basis of immigration enforcement, and the government does not seriously contend otherwise. *See* Gov't Br. 40-41 n.18; Addendum 20. This is particularly true here where Plaintiffs—U.S. citizens and lawful permanent residents—are, by definition, admissible. Addendum 20-21. Rather, the only possible government interest that could justify application of the border search exception to searches of digital devices is the interdiction of contraband. *See Montoya de Hernandez*, 473 U.S. at 544 (customs enforcement intended to prevent entrants from "bring[ing] anything harmful into this country"). That interest is attenuated in the context of digital devices.

Digital devices store intangible data, not the physical contraband that historically has justified the border search exception. As the Fourth Circuit recently noted, such devices "store vast quantities of uniquely sensitive and intimate personal

information, … yet cannot contain many forms of contraband, like drugs or firearms, the detection of which constitutes the strongest historic rationale for the border-search exception." *United States v. Aigbekaen*, 943 F.3d 713, 721 (4th Cir. 2019) (cleaned up)). As a result, "the detection-of-contraband justification would rarely seem to apply to an electronic search of a cell phone outside the context of child pornography." *Cano*, 934 F.3d at 1021 n.13.

The questionable efficacy of border searches of digital devices further undermines the government's interest. The government claims that such searches have uncovered threats and plots, but "without explanation of the frequency, nature of same or the manner of the discovery of same," this contention "is not a strong counterweight to the intrusion on personal privacy." Addendum 20. In other words, the government has failed to show "that the ability to conduct a warrantless search would make much of a difference." *Riley*, 573 U.S. at 390. There is good reason to be skeptical that application of the border search exception would make much of a difference because digital contraband can be transmitted across borders via the Internet.[31]

Several courts have recognized that the traditional rationales for the border exception are less applicable to searches of digital devices, which often uncover

[31] *See, e.g.*, Hardy, *supra*, note 23 (digital devices make use of "cloud computing systems … that span the globe").

"merely indirect evidence" of criminality rather than digital contraband. *United States v. Kolsuz*, 185 F. Supp. 3d 843, 858 (E.D. Va. 2016) (government's interest in obtaining "indirect evidence of the things an individual seeks to export illegally—not the things themselves—… is less significant than the government's interest in directly discovering the items to be exported illegally."), *aff'd*, 890 F.3d 133 (4th Cir. 2018). "There is a difference between a search for contraband and a search for evidence of border-related crimes." *Cano*, 934 F.3d at 1017. Border agents are authorized to seize contraband, but "border officials have no general authority to search for crime." *Id.* Thus, searches of digital devices easily can exceed the scope of the border search exception.

In sum, searches of digital devices do "not possess the characteristics of a border search or other regular inspection procedures"; instead, they "more resemble the common non-border search based on individualized suspicion, which must be prefaced by the usual warrant and probable cause standards." *United States v. Kim*, 103 F. Supp. 3d 32, 57-58 (D.D.C. 2015).

D. Balancing the Privacy Interests at Stake Against the Government's Attenuated Interests, This Court Should Impose a Warrant Requirement on Border Searches of Digital Devices.

This Court should hold that a warrant is required for searches of digital devices at the border because the paramount privacy interests at stake outweigh the government's attenuated interests. "On the government interest side," the

justifications that underpin the border search do not apply "when the search is of digital data"; at the same time, digital devices "implicate privacy concerns far beyond those implicated by the search of" a traveler's physical belongings. *Riley*, 573 U.S. at 386, 393. In other words, the government's interests in border searches of digital devices are too attenuated to justify destroying an individual's privacy interest in the sensitive information they store.

A warrant requirement is an easy-to-administer, bright-line rule that does not unjustifiably burden the government. Border agents have tools at their disposal to secure digital devices while a warrant is secured. A "warrant process will not significantly increase the delay before" a digital device can be searched because a border agent "can take steps to secure a warrant" while the device is screened and secured. *Missouri v. McNeely*, 569 U.S. 141, 153-54 (2013). As the District Court found, border agents can make use of investigatory stops during primary and secondary inspections to determine whether a search of a digital device is needed and make preparations to secure a warrant. Addendum 38. This is particularly true in light of "technological developments in warrant procedures," which mitigate any delay. *McNeely*, 569 U.S. at 156. In such circumstances, there is "no plausible justification for an exception to the warrant requirement." *Id*. at 153-54. Moreover, if faced with a true threat or emergency, the government can rely on the exigent circumstances exception to the warrant requirement. *Riley*, 573 U.S. at 402.

Courts have required warrants for searches of digital devices in myriad contexts, recognizing the privacy intrusion of such searches. For example, in *United States v. Lara*, the Ninth Circuit found that a warrantless search of probationer's cellphone was unreasonable even where the probationer had consented to searches and had a lessened expectation of privacy, because the interest "was nonetheless sufficiently substantial" given the "importance of cell phone privacy." 815 F.3d 605, 609-12 (9th Cir. 2016); *see also United States v. Hulscher*, 2017 WL 657436, at *2-3 (D.S.D. Feb. 17, 2017) (requiring the government to apply for warrant to search cellphone data already collected by another law enforcement organization due to the "immense amounts of information" contained on cellphones).

In requiring a warrant to search digital devices, courts have reasoned that such devices are unlike other containers or items on which prior deviations from the Fourth Amendment's warrant requirement were based. *See, e.g.*, *United States v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009) ("Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."). And the Supreme Court has warned that "[t]reating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter," "[b]ut the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen." *Riley*, 573 U.S. at 397.

Other courts have found that a search of digital devices requires a warrant based on the nature of the physical intrusion involved. In *United States v. Sam*, the court concluded that simply powering on a cellphone required a warrant because "when the Government gains evidence by physically intruding on a constitutionally protected area ... it is 'unnecessary to consider' whether the government also violated the defendant's reasonable expectation of privacy." 2020 WL 2705415, at *2 (W.D. Wash. May 18, 2020) (quoting *Florida v. Jardines*, 569 U.S. 1, 10-11 (2013)).

Permitting border searches of digital devices without a warrant would not adequately protect the privacy interests of individuals. Rapid technological developments create a "[gap] between the well-established rules lower courts have and the ones they need in the realm of technology." *In re Cellular Telephones*, 2014 WL 7793690, at *4 (D. Kan. Dec. 30, 2014). Courts must close this gap by "resisting the temptation to rationalize the application of ill-fitting precedent to circumstances," *id*., so as to not compromise the values enshrined in the Fourth Amendment, *see Riley*, 573 U.S. at 403 ("The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.").

Ultimately, *Riley* is instructive and should be followed. That "the Supreme Court has specifically likened the border search warrant exception to the search incident to arrest exception reinforces" the need to hew closely to *Riley*'s reasoning.

Kim, 103 F. Supp. 3d at 55 (citing *Ramsey*, 431 U.S. at 621). In narrowing the search-incident-to-arrest exception and requiring a warrant—not reasonable suspicion—the Court demonstrated that warrant exceptions must be redrawn to account for the fact that digital devices "hold for many Americans 'the privacies of life.'" *Riley*, 573 U.S. at 403 (quoting *Boyd*, 116 U.S. at 630). As in *Riley*, the governmental interest in searches of digital devices at the border is too attenuated to justify this unreasonable invasion of privacy. Accordingly, this Court should require a warrant for border searches of digital devices.

III. The District Court Correctly Found That, at a Minimum, the Government's Border Search Policies Permitting Suspicionless Manual Searches Violate the Fourth Amendment.

The balance of the privacy interests at stake against the Government's attenuated interests should compel this Court to conclude that a warrant is required for all border searches of digital devices. But if the Court determines that warrants are not required, it should—as the District Court held—require reasonable suspicion of digital contraband for both manual and forensic searches of digital devices at the border.

The District Court correctly reasoned that because manual and forensic searches both can "reveal a wealth of personal information," there is no "meaningful difference between the two classes of searches in terms of the privacy interests implicated." Addendum 30. Accordingly, just as forensic searches require at least

reasonable suspicion—which the Government concedes—it follows that manual searches also should require at least reasonable suspicion that the device at issue contains digital contraband.

The Government argues that the District Court's reasoning is "divorced from practical reality." Gov't Br. at 36. To the contrary, the District Court correctly understood the practical realities implicated here. Manual searches can be extremely intrusive because digital devices store private information that can be easily accessed through a manual search. *See*, *supra*, section I. For many digital devices such as smartphones, no external equipment is needed to uncover every detail of an individual's private life. Moreover, there is no time limit to manual searches. Thus, using simple keyword searches and the common applications found on digital devices described above, border agents can sift through all the private information stored on such devices at an efficient, targeted pace.

The government's policies allow border agents essentially unfettered discretion to rummage through the "vast quantities of personal information" contained in a digital device, *Riley*, 573 U.S. at 386, with little to no legal protections. The Fourth Amendment does not permit such invasive suspicionless searches. *See Aigbekaen*, 943 F.3d at 722; *Cano*, 934 F.3d at 1018; *Kim*, 103 F. Supp. 3d at 57. The District Court was correct to hold that, at a minimum, manual searches require reasonable suspicion that the device searched contains digital contraband.

CONCLUSION

For the foregoing reasons, this Court should hold that a warrant is required for both manual and forensic searches of digital devices at the border; or, at a minimum, affirm that both manual and forensic searches of digital devices at the border require reasonable suspicion that a device contains digital contraband.

Respectfully submitted,

/s/Rafael Reyneri
Kurt Wimmer
Rafael Reyneri
Calvin Cohen
Frank Broomell
COVINGTON & BURLING LLP
850 Tenth Street, NW
Washington, DC 20001
(202) 662-6000
rreyneri@cov.com

Counsel for Amici Curiae

August 17, 2020

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing Brief complies with the type-volume limitations of Rule 29(a)(5) of the Federal Rules of Appellate Procedure because it contains 6,477 words, excluding the parts of the brief exempted by Rule 32(f). I further certify that this Brief complies with the typeface requirements of Rule 32(a)(5) and the type-style requirements of Rule 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman font.

/s/Rafael Reyneri

August 17, 2020

CERTIFICATE OF SERVICE

I hereby certify that on August 17, 2020, I caused the foregoing Brief to be filed with the Clerk of the U.S. Court of Appeals for the First Circuit using the appellate CM/ECF system and to be served upon counsel for all parties via the CM/ECF system.

/s/Rafael Reyneri