No. 17-50070

UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

UNITED STATES OF AMERICA

Plaintiff–Appellee,

v.

MARIA ISABEL MOLINA-ISIDORO

Defendant–Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TEXAS, EL PASO DIVISION

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, ACLU OF TEXAS, ACLU OF LOUISIANA, AND ACLU OF MISSISSIPPI IN SUPPORT OF DEFENDANT-APPELLANT SEEKING REVERSAL

Edgar Saldivar
Texas Bar No. 24038188
ACLU Foundation of Texas
1500 McGowen St., Ste. 250
Houston, TX 77004
Phone: 713-942-8146
Fax: 713-942-8966
esaldivar@aclutx.org

Kali Cohn
Texas Bar. No. 24092265
ACLU Foundation of Texas
6440 N. Central Expressway
Dallas, TX 75206

Esha Bhandari
Nathan Freed Wessler
Vera Eidelman
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ebhandari@aclu.org

Phone: 214-346-6577
Fax: 713-942-8966
kcohn@aclutx.org

Bruce Hamilton
ACLU Foundation of Louisiana
P.O. Box 56157
New Orleans, LA 70156
Phone: (504) 522-0628
Fax: (504) 613-6511
bhamilton@laaclu.org

Paloma Wu
ACLU of Mississippi Foundation
233 East Capitol Street
Jackson, MS 39201
Phone: 601-354-3408
Fax: 601-355-6465
pwu@aclu-ms.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

STATEMENT REGARDING ORAL ARGUMENT

Amici curiae submit that oral argument is appropriate in this case because the Fourth Amendment question on appeal is unresolved in this Circuit. *Amici curiae* respectfully seek leave to participate in oral argument on the constitutional implications of the district court's erroneous ruling because their participation may be helpful to the Court in addressing the novel and important issues presented by this appeal. See Fed. R. App. P. 29(a)(8). Defendant-Appellant consents and joins in this request.

SUPPLEMENTAL STATEMENT OF INTERESTED PARTIES

Pursuant to Fifth Circuit Rule 29.2, the undersigned counsel of record for *amici curiae* certifies that the following additional persons and entities have an interest in the outcome of this case.

1. The American Civil Liberties Union, the American Civil Liberties Union of Texas, the American Civil Liberties Union of Louisiana, and the American Civil Liberties Union of Mississippi. *Amici curiae* are non-profit organizations that have no parent corporations, and no publicly held corporation owns 10 percent or more of their stock.
2. Esha Bhandari, Nathan Freed Wessler, Vera Eidelman, Edgar Saldivar, Kali Cohn, Bruce Hamilton, and Paloma Wu, attorneys for *amici curiae*.

Dated: August 22, 2017 *<u>/s/ Esha Bhandari</u>*

Esha Bhandari

INTEREST OF AMICI CURIAE[1]

The American Civil Liberties Union ("ACLU") is a nationwide, non-profit, non-partisan organization of more than 1 million members dedicated to defending the civil liberties guaranteed by the Constitution. The ACLU of Texas, the ACLU of Louisiana, and the ACLU of Mississippi are state affiliates of the national ACLU. The ACLU has been at the forefront of numerous state and federal cases addressing the right of privacy as guaranteed by the Fourth Amendment.

[1] Defendant-Appellant consents to the filing of this *amicus* brief. Plaintiff-Appellee United States leaves acceptance of this *amicus* brief to the Court's discretion. Pursuant to Fed. R. App. P. 29(a)(3), counsel for *amici curiae* have therefore submitted a motion for leave to file this brief. In addition, counsel for *amici curiae* certifies that no counsel for a party authored this brief in whole or in part, and no person other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission.

SUMMARY OF ARGUMENT

This case presents an important question about the extent of Fourth Amendment privacy rights in the digital age, where the use of mobile devices is widespread. The government's assertion of authority to search such devices without any individualized suspicion when an individual is crossing the border—whether entering or leaving the United States—creates an end-run around Fourth Amendment protections that would otherwise apply to the voluminous and intimate information contained in those devices, and is not justified by the rationale permitting routine border searches.

Millions of people cross the United States' borders every year for school, business, pleasure, and family obligations. Large numbers of those travelers carry laptops, smartphones, and other portable electronic devices that, despite their small size, have "immense storage capacity." *Riley v. California*, 134 S. Ct. 2473, 2489 (2014). The information on these devices can be deeply sensitive and private, including personal correspondence, notes and journal entries, family photos, medical records, lists of associates and contacts, proprietary or privileged business information, attorney-client communications, and more. This information can be stored on the device itself, or contained in cloud-based accounts that are accessible from the device. The Department of Homeland Security itself recognizes that border searches of electronic devices raise "unique privacy concerns," unlike those

inherent in searches of other luggage.[2] Nevertheless, the government claims the right to seize these devices at the border, detain them, and invasively search them with no warrant or individualized suspicion whatsoever.

This Court should affirm that *Riley* squarely governs this case, because the search of the defendant's electronic device took place after her arrest. *Riley* imposes a warrant requirement for such searches incident to arrest of electronic devices, and no loophole in this requirement is justified simply because the arrest took place at a border. Should this Court decide, however, that the jurisprudence governing border searches applies in this case, it should take the opportunity to clarify the Fourth Amendment standards governing such searches given the significant privacy interests at stake. This Court should hold that searches of electronic devices may not be conducted without a warrant or, at an absolute minimum, a determination of probable cause. This Court should so hold even if it determines that the government had the requisite level of suspicion in this case. In light of evidence that the number of device searches at the border is increasing, the failure to articulate the appropriate standard may result in a "significant diminution of privacy" for travelers. *Riley*, 134 S. Ct. at 2493.

---

[2] U.S. Dep't of Homeland Sec., *Privacy Impact Assessment for the Border Searches of Electronic Devices* (2009), *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf.

ARGUMENT

I. The Search at Issue Was Incident to Arrest and Therefore Required a Warrant.

The Supreme Court squarely held in *Riley v. California* that the government must obtain a warrant before searching digital information on a cell phone seized from someone who has been arrested. 134 S. Ct. at 2495. The *Riley* holding dictates the outcome here, as there is no dispute that border agents searched the defendant's cell phone *after* arresting her at a port of entry and advising her of her *Miranda* rights. *See United States v. Molina-Isidoro*, No. 16-1402, 2016 WL 8138926, at *2 (W.D. Tex. Oct. 7, 2016). The government's attempt to argue for a more lenient standard under the Fourth Amendment, simply because of the location of the arrest, constitutes an end-run around the holding and rationale of *Riley*.

The border search exception to the warrant requirement does not apply in circumstances like this one. Once the defendant was arrested, any search of her cell phone was no longer a search conducted "in order to regulate the collection of duties and to prevent the introduction of contraband." *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). Border agents already had discovered that the defendant was carrying contraband and determined that they had probable cause to arrest her on a criminal charge. Their post-arrest search for evidence regarding that charge on the defendant's cell phone is not the type of routine, or

even non-routine, search for which the border search exception to the warrant requirement developed; the search did not serve "[t]he Government's interest in preventing the entry of unwanted persons and effects," *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004), but rather its interest in collecting evidence for the prosecution of an arrested criminal suspect. Accordingly, the search of the defendant's cell phone required a warrant, per *Riley*, and this Court should reverse the district court's denial of the motion to suppress the search.

II. Border Searches of Electronic Devices Raise Serious Privacy Concerns and Are Subject to Fourth Amendment Protections.

Amici believe that the district court erred in treating this search as a "border search" rather than an ordinary criminal investigatory search. Should this Court disagree, it should nonetheless recognize the serious privacy implications of permitting the government to search and seize a person's electronic device at the border without individualized suspicion. The number of border searches of electronic devices is increasing rapidly, and the privacy concerns such searches raise are acute.

A. Border Searches of Electronic Devices Are Increasing Rapidly.

Each year, millions of people travel through border crossings, international airports, and other ports of entry into the United States.[3] Of those, hundreds of thousands of travelers undergo secondary screenings, and thousands of individuals have their electronic devices confiscated, detained, and searched. *See* Cynthia McFadden et al., *American Citizens: U.S. Border Agents Can Search Your Cellphone*, NBC News, Mar. 13, 2017, http://www.nbcnews.com/news/us-news/american-citizens-u-s-border-agents-can-search-your-cellphone-n732746 [hereinafter "McFadden"] (identifying 19,033 electronic device searches in 2016 based on data provided by the government). The Department of Homeland Security has justified its practice of searching electronic devices in part by noting "how infrequent[ly such] searches are conducted,"[4] but border searches of

---

[3] U.S. Dep't of Homeland Sec., *Civil Rights/Civil Liberties Impact Assessment: Border Searches of Electronic Devices* 1 (2011), http://www.dhs.gov/sites/default/files/publications/Redacted%20Report.pdf [hereinafter "DHS CR/CL Impact Assessment"] (reporting monthly average of 29,357,163 travelers in fiscal year 2010); *see also* Tal Kopan, *First on CNN: Senator Seeks Answers on Border Cell Phone Searches*, CNN, Feb. 20, 2017, http://www.cnn.com/2017/02/20/politics/border-search-cell-phones-ron-wyden-dhs-letter/ ("In fiscal year 2016, 390 million people entered the [United States] . . . .").

[4] *See* Mary Ellen Callahan, U.S. Dep't of Homeland Sec., *Privacy Issues in Border Searches of Electronic Devices* (2009), https://www.dhs.gov/sites/default/files/publications/privacy_privacy_issues_border_searches_electronic_devices.pdf.

electronic devices more than doubled in 2016. *See* McFadden (noting that electronic device searches rose from 8,503 in 2015 to 19,033 in 2016).

B. Searches of Travelers' Electronic Devices Pose Serious Privacy Concerns.

The government claims the authority to search international travelers' electronic devices without any particularized or individualized suspicion, let alone a search warrant or probable cause. U.S. Customs and Border Protection ("CBP") and U.S. Immigration and Customs Enforcement ("ICE") both have formal policies permitting border officials to read and analyze information on electronic devices without a warrant or individualized suspicion[5]—including legal or privileged information, information carried by journalists, medical information, confidential business information, and other sensitive information. ICE policy states that "a claim of privilege or personal information does not prevent the search of a traveler's information at the border." ICE Policy § 8.6(1). Under CBP policy, an officer or agent "may be subject" to the requirement that he "seek advice" from

---

[5] U.S. Customs and Border Protection, *Border Search of Electronic Devices Containing Information*, Directive No. 3340-049, § 5.1.2 (Aug. 20, 2009), http://www.dhs.gov/sites/default/files/publications/cbp_directive_3340-049%20Homeland%20directive_0.pdf\ [hereinafter "CBP Policy"]; U.S. Immigration and Customs Enforcement, *Border Searches of Electronic Devices*, Directive No. 7-6.1 § 6.1 (Aug. 18, 2009), http://www.dhs.gov/sites/default/files/publications/7-6.1%20directive.pdf [hereinafter "ICE Policy"].

counsel before accessing "legal materials," but CBP does not require officials to seek such advice. CBP Policy § 5.2.1.

These policies have been reaffirmed in recent years, both in policy documents, *see, e.g.*, DHS CR/CL Impact Assessment ("[W]e are not recommending that officers demonstrate reasonable suspicion for the device search . . . ."), and in litigation filings.[6] The effect of these policies is significant, both because of the number of international travelers, and because of the volume and variety of sensitive information contained on or accessible from their electronic devices.

Use of mobile, or portable, electronic devices is pervasive. Nearly every American adult owns a cell phone of some kind. *See* Pew Research Ctr., *Mobile Fact Sheet* (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/ [hereinafter "Pew Mobile Fact Sheet] (noting 95 percent prevalence today); *Riley*, 134 S. Ct. at 2490 (90 percent prevalence in 2014). Today, 77 percent of American adults own a smartphone, and rates of smartphone ownership are even higher among younger Americans[7]—who travel internationally at increasingly high rates.[8]

---

[6] *See, e.g.*, Br. of Appellee, *United States v. Vergara*, No. 16-15059, 2017 WL 360182, at *14–17 (11th Cir. Jan. 23, 2017).

[7] Pew Mobile Fact Sheet.

People rely on these devices for communication (via text messages, calls, email, and social networking), navigation, entertainment, news, photography, and a multitude of other functions.[9] In addition, more than ten percent of American adults use a smartphone as their sole means of accessing the internet at home, meaning that everything they do online—from sending email to searching Google to banking—may be accessible through a single mobile electronic device.[10] Other types of mobile electronic devices also have high rates of use: more than 80 percent of U.S. households have a laptop computer and 54 percent own a tablet.[11]

People consistently carry these devices with them, including when they travel. Indeed, "[a]ccording to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting

---

[8] Tanya Mohn, *Travel Boom: Young Tourists Spent $217 Billion Last Year, More Growth Than Any Other Group*, Forbes, Oct. 7, 2013, http://www.forbes.com/sites/tanyamohn/2013/10/07/the-new-young-traveler-boom/.

[9] *See, e.g.*, Aaron Smith, Pew Research Ctr., *U.S. Smartphone Use in 2015, Chapter Three: A "Week in the Life" Analysis of Smartphone Users* (2015), http://www.pewinternet.org/2015/04/01/chapter-three-a-week-in-the-life-analysis-of-smartphone-users/.

[10] Pew Mobile Fact Sheet.

[11] Deloitte, *Digital Democracy Survey* 5 (9th ed. 2015), http://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-DDS_Executive_Summary_Report_Final_2015-04-20.pdf.

that they even use their phones in the shower." *Riley*, 134 S. Ct. at 2490. Mobile devices serve "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 . . . ." *United States v. Saboonchi*, 990 F. Supp. 2d 536, 557–58 (D. Md. 2014). Moreover, a person who travels with one electronic device often will travel with several, thus multiplying the digital data in their possession. *See, e.g.*, *United States v. Hassanshahi*, 75 F. Supp. 3d 101, 107 (D.D.C. 2014) (discussing seizure of traveler's "laptop computer, multimedia cards, thumb drives, a camcorder, SIM cards, and a cell phone").

When a traveler's electronic device is searched at the border, the intrusion can be severe because a computer "is akin to a vast warehouse of information." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005). A decade ago, a typical commercially available 80-gigabyte hard drive could carry data "roughly equivalent to forty million pages of text—about the amount of information contained in the books on one floor of a typical academic library." *Id.* at 542; *see also United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1175 (9th Cir. 2010) (en banc) ("[E]ven inexpensive electronic storage media today can store the equivalent of millions of pages of information."). Today's devices are even more capacious. Laptops for sale in 2017 can store up to

two terabytes,[12] the equivalent of more than 1.3 billion pages of text.[13] Even tablet computers can be purchased with a terabyte of storage.[14]

Smartphones also provide large storage capacities and can hold the equivalent of "millions of pages of text, thousands of pictures, or hundreds of videos." *Riley*, 134 S. Ct. at 2489. Moreover, the availability of cloud-based storage, email, and social media services can increase exponentially the functional capacity of a device.[15]

Not only do electronic devices contain or provide access to great quantities of data, they also contain a diverse array of information—much of it exceedingly sensitive. As the Supreme Court explained in *Riley*, cell phones are "minicomputers that . . . could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." 134 S. Ct. at 2489; *see also United States v. Cotterman*, 709 F.3d

---

[12] *See* Apple, *Compare Mac models*, https://www.apple.com/mac/compare/ (last visited August 21, 2017).

[13] *See* LexisNexis, *How Many Pages in a Gigabyte?* (2007), http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf.

[14] *See* Microsoft, *Surface Pro 4*, https://www.microsoft.com/en-us/surface/devices/surface-pro-4/overview (last visited August 21, 2017).

[15] *See, e.g.*, Google, *Pricing Guide*, https://www.google.com/drive/pricing/ (last visited August 21, 2017) (offering up to 10 terabytes of paid cloud storage).

952, 964 (9th Cir. 2013) (en banc) ("Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain . . . financial records, confidential business documents, medical records and private emails."). Many categories of information that courts have recognized as deserving of particularly stringent privacy protections can be contained on people's mobile devices, including internet browsing history,[16] medical records,[17] historical cell phone location data,[18] email,[19] privileged communications,[20] and associational information.[21]

---

[16] *See Riley*, 134 S. Ct. at 2490 ("An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

[17] *See Ferguson v. Charleston*, 532 U.S. 67, 78 (2001) (expectation of privacy in diagnostic test results).

[18] *See Riley*, 134 S. Ct. at 2490 ("Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.").

[19] *See United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) ("[E]mail requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve.").

[20] *See Jaffee v. Redmond*, 518 U.S. 1, 15 (1996) (psychotherapist-patient privilege); *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981) (attorney-client privilege); *Blau v. United States*, 340 U.S. 332, 333 (1951) (marital communications privilege).

[21] *Riley*, 134 S. Ct. at 2490 ("Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of

The data contained on mobile devices is also particularly sensitive because it does not represent merely isolated snapshots of a person's life, but can span years; indeed, "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions" or a "record of all [a person's] communications." *Riley*, 134 S. Ct. at 2489. Much of the private data that can be accessed in a search of a mobile device has no analogue in pre-digital searches because it never could have been carried with a person, or never would have existed at all. This includes deleted items that remain in digital storage unbeknownst to the device owner, historical location data, cloud-stored information, metadata about digital files created automatically by software on the device, and password-protected or encrypted information. *Riley*, 134 S. Ct. at 2490–91; *Cotterman*, 709 F.3d at 965.

Any search of a mobile device therefore implicates serious privacy interests. *Riley*, 134 S. Ct. at 2488–91. Furthermore, a regime of suspicionless device searches implicates First Amendment freedoms. In the closely-related context of customs searches of incoming international mail, the Supreme Court recognized

---

a person's life. There are apps for Democratic Party news and Republican Party news . . . ."); *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958) ("[C]ompelled disclosure of affiliation with groups engaged in advocacy may constitute . . . a restraint on freedom of association . . . .").

that First Amendment-protected speech might be chilled by such searches. While the Court declined to invalidate the existing search regime, it notably did so because of regulations "flatly prohibit[ing], under all circumstances" customs officials from reading correspondence without a search warrant. *United States v. Ramsey*, 431 U.S. 606, 623 (1977). The Supreme Court explicitly left open the question of whether, "in the absence of the existing statutory and regulatory protection," "the appropriate response [to a chill on speech] would be to apply the full panoply of Fourth Amendment requirements." *Id*. at 624 & n.18. Notably, the government recognizes no similar restriction on reading the information accessible on an electronic device seized at the border, even though the chill on First Amendment rights may be even greater because of the quantity and quality of information contained.

These privacy and First Amendment concerns are implicated regardless of whether border officials do a "manual" search of a device, or a so-called "forensic" search. In the case of manual searches, the existence of cloud-based services on smartphones—including email, social media, financial, or health services—means that even a brief search of a mobile device could allow a government agent access

to a vast trove of private information.[22] Even without accessing cloud-stored data, an officer without specialized training or equipment can conduct keyword searches using the device's built-in search function, thereby achieving many of the goals of a forensic search with a fraction of the effort.[23] For these reasons, Fourth Amendment protections should apply no less robustly to manual searches of electronic devices than to "forensic" searches of electronic devices.

Forensic and similar searches, too, are highly invasive. Forensic searches typically begin with an agent making a mirror-image copy of a device's entire hard drive or other digital storage repository, including all active files, deleted files,[24] allocated and unallocated file space,[25] metadata, and password-protected or

---

[22] In July 2017, CBP publicly announced that its agents are not supposed to access cloud-stored data during border searches of electronic devices. The search at issue in this case took place prior to this public statement by CBP. *See* E.D. Cauchi, *Border Patrol Says It's Barred From Searching Cloud Data on Phones*, NBC News, July 12, 2017, http://www.nbcnews.com/news/us-news/border-patrol-says-it-s-barred-searching-cloud-data-phones-n782416.

[23] *See, e.g.*, Apple, *iPhone 7: iOS 10*, https://www.apple.com/iphone-7/ios/ (last visited August 21, 2017) ("When you search your photo collection, Photos performs billions of calculations to identify images with the specific people, places, and things you're looking for.").

[24] "[M]arking a file as 'deleted' normally does not actually delete the file; operating systems do not 'zero out' the zeros and ones associated with that file when it is marked for deletion." Kerr, 119 Harv. L. Rev. at 542.

[25] "'Unallocated space is space on a hard drive that contains deleted data . . . that cannot be seen or accessed by the user without the use of forensic software.'" *Cotterman*, 709 F.3d at 958 n.5 (citation omitted).

encrypted data. *See* Nat'l Inst. of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* 16 (2004), https://www.ncjrs.gov/pdffiles1/nij/199408.pdf. That copy is then analyzed using powerful programs that read and sort every file and byte stored on the device, including deleted files and other files that the device user may not even be aware exist.

The forensic search tools used by the government can extract and analyze tremendous quantities of data.[26] In one recent case, for example, an agent "employed a software program called EnCase . . . to export six Microsoft Outlook email containers[, that can each contain thousands of email messages], 8,184 Microsoft Excel spreadsheets, 11,315 Adobe PDF files, 2,062 Microsoft Word files, and 879 Microsoft PowerPoint files," as well as "approximately 24,900 .jpg [picture] files," from a laptop. *United States v. Kim*, 103 F. Supp. 3d 32, 40–41 &

---

[26] Forensic searches are not the only way to uncover large quantities of sensitive data from an electronic device. *See United States v. Kim*, 103 F. Supp. 3d 32, 55 (D.D.C. 2015) ("[T]he analysis of whether the search of Kim's laptop was reasonable under the Fourth Amendment . . . does not turn on the application of an undefined term like 'forensic.'"). The government could also, for example, download a program onto the device itself to search deleted files and other hard-to-access information without first making a forensic copy. *See, e.g.*, Piriform, *Recuva*, https://www.piriform.com/recuva (last visited August 21, 2017) ("Recuva has an advanced deep scan mode that scours your drives to find any traces of files you have deleted.").

n.3 (D.D.C. 2015). Any time a device seized at the border remains in government custody, it is potentially subject to a forensic search.

Border searches of electronic devices allow government agents to read and analyze all of the vast amount of data stored on a mobile device with little time and effort. *See generally Cotterman*, 709 F.3d 952. In effect, such searches allow the government to learn "not just one [sensitive] fact about a person, but all such facts." *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom. United States v. Jones*, 132 S. Ct. 945 (2012).

C. This Court Should Ensure that the Protections of the Fourth Amendment Are Not Eroded by Advancing Technology.

This Court should address the serious threat to privacy posed by warrantless, suspicionless searches of travelers' electronic devices. Without an explanation of how the Fourth Amendment applies to these searches, the protections of the Constitution risk becoming a dead letter for the millions of people who cross the nation's borders each year.

The Supreme Court has cautioned that new technologies should not be allowed to "erode the privacy guaranteed by the Fourth Amendment." *Kyllo v. United States*, 533 U.S. 27, 34 (2001); *see also United States v. Warshak*, 631 F.3d 266, 285 (6th Cir. 2010) ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."). Indeed, the district court's opinion in this case highlights the need for

this Court's guidance. The district court noted that "there is no Fifth Circuit precedent regarding border searches of technology—such as cell phones" but nonetheless determined that it could not decide the question "in the first instance" absent instruction from a higher court. *See Molina-Isidoro*, 2016 WL 8138926, at *8 (acknowledging that the rationale of *Riley* could one day lead the Supreme Court to apply a warrant requirement to searches of electronic devices at the border and noting that "were [the court] free to decide this matter in the first instance, it might prefer that a warrant be required to search an individual's phone at the border"). Only one court of appeals has addressed the important constitutional question raised in this case, *see Cotterman*, 709 F.3d at 960, and that court did so before the Supreme Court decided *Riley*, which counsels adoption of a more privacy-protective rule than the *Cotterman* court contemplated. Other district courts grappling with this question have reached different results. *Compare Kim*, 103 F. Supp. 3d at 54–59 (holding that a border search of electronic devices requires some level of individualized suspicion), *with United States v. Feiten*, No. 15-20631, 2016 WL 894452, at *4–7 (E.D. Mich. Mar. 9, 2016) (holding the opposite). This Court should take up the mantle of ensuring that the Fourth Amendment is not allowed to atrophy in the face of rapid technological change.

Guidance from this Court is also important to ensure that government agents do not take the wrong lessons from prior holdings of this Court that are not binding

and do not clearly apply here. In particular, *United States v. Escarcega*, No. 15-51090, 2017 WL 1380555 (5th Cir. Apr. 17, 2017), should not be read to justify suspicionless border searches of electronic devices. The unpublished opinion is not binding on this Court, *see* Fifth Cir. R. 47.5.4, and it fails to offer sufficient guidance on the requisite Fourth Amendment standard. While *Escarcega* held that a search of a phone conducted at the border was "constitutionally valid" notwithstanding *Riley* "because of the difference between a simple arrest and the plenary power of customs officials to search for concealed merchandise," the opinion failed to clarify whether the search was conducted with or without a warrant. *See Escarcega*, 2017 WL 1380555, at *1 (initially describing the search as "warrantless" but then stating that the border control officers "obtained a warrant" before "[going] through the phone's content to obtain incriminating evidence"). To guide lower courts, this Court should make clear that neither the facts nor reasoning of *Escarcega* justify suspicionless border searches of electronic devices.

III. Searches of Electronic Devices Seized at the Border Require a Warrant or Probable Cause.

As the Supreme Court has repeatedly declared, "'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.'" *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). Among those

exceptions are search incident to arrest,[27] search pursuant to exigent circumstances,[28] vehicular search,[29] and border search.[30] But none of these exceptions apply automatically upon invocation; rather, they must remain "[]tether[ed]" to "the justifications underlying the . . . exception." *Gant*, 556 U.S. at 343 (holding that the search-incident-to-arrest exception does not permit all warrantless searches of an arrestee's vehicle); *accord Riley*, 134 S. Ct. at 2484 (holding that the search-incident-to-arrest exception does not apply to searches of cell phones because "neither of its rationales has much force with respect to digital content on cell phones"). As relevant to this case, the border search exception does not cover the highly invasive search of smartphones, laptops, and other portable electronic devices. "[A]ny extension of that reasoning to digital data has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489.

As the Supreme Court explained in *Ramsey*, the border search exception "is a longstanding, historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained, and in this respect is like the similar 'search incident to lawful arrest' exception." 431 U.S. at 621. Like other

---

[27] *United States v. Robinson*, 414 U.S. 218 (1973).

[28] *Mincey v. Arizona*, 437 U.S. 385 (1978).

[29] *California v. Acevedo*, 500 U.S. 565 (1991).

[30] *United States v. Flores-Montano*, 541 U.S. 149 (2004).

exceptions to the warrant requirement, including searches incident to arrest, the reasonableness of a border search is determined by balancing the government's relevant interests against the individual's privacy interest. *See Riley*, 134 S. Ct. at 2484; *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999); *Montoya de Hernandez*, 473 U.S. at 539. This Court must therefore balance the interests at stake, and should look to *Riley*'s analysis for guideposts in how to conduct such balancing. In *Riley*, the Supreme Court concluded that the significant privacy interests implicated by searches of cell phones outweigh the governmental interests in officer safety and preservation of evidence that underlie the search-incident-to-arrest exception. 134 S. Ct. at 2495. This holding counsels that a warrant should be required for searches of electronic devices at the border.

The government's interest in border search cases is "the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country." *Ramsey*, 431 U.S. at 616. Therefore, on the government's side of the balance is its "interest in preventing the entry of unwanted persons and effects [which] is at its zenith at the international border." *Flores-Montano*, 541 U.S. at 152. While the balance is generally "struck much more favorably to the Government" as a result, *Montoya de Hernandez*, 473 U.S. at 540, the government's interest is limited to determining the admissibility of individuals and preventing the transport of contraband.

On the other side of the balance, the individual privacy interest in the contents of a smartphone or laptop is extraordinarily strong. *See Riley*, 134 S. Ct. at 2491 ("[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house."); *Cotterman*, 709 F.3d at 960 ("Even at the border, individual privacy rights are not abandoned.").[31] Engaging in this balancing exercise has led at least one district court to conclude that, even at the border, the *Riley* opinion "strongly indicate[s] that a digital data storage device cannot fairly be compared to an ordinary container when evaluating the privacy concerns involved." *Kim*, 103 F. Supp. 3d at 55.

The individual's interest is also strong because of the duration of the interference with Fourth Amendment rights. *Cf. United States v. Place*, 462 U.S. 696, 708-10 (1983) (length of detention of a traveler's luggage is an "important factor" in determining level of suspicion required). When it copies the entire contents of a device and holds onto the copy indefinitely, the government effects a permanent seizure under the Fourth Amendment. Creating, searching, and storing the copy divests a person of two important property rights: the right to exclude others, and the right to dispose of property. The initial copying constitutes a seizure

[31] The privacy harms inflicted by forensic and forensic-like searches surpass even what the *Riley* Court contemplated. *See supra* Part II.B.

for which a warrant is required, and as long as the government retains the copy, the intrusion on Fourth Amendment interests continues. *See Comprehensive Drug Testing*, 621 F.3d 1162 (referring to the copying of electronic data as a "seizure"). The indefinite duration of the seizure necessitates a greater level of protection under the Fourth Amendment. *See United States v. Laich*, No. 08-20089, 2010 WL 259041, at *4 (E.D. Mich. Jan. 20, 2010) (permanent seizure of a laptop at the border followed by its transportation hundreds of miles away required probable cause).

The privacy interests must be balanced against the government's particular border-related interest in searching the contents of electronic devices, which interest is lower than the government's interest in searching luggage for contraband or dangerous items. In *Ramsey,* the Supreme Court concluded that searching envelopes at the border is justified when "the customs officers have reason to believe they contain *other than* correspondence, while the reading of any correspondence inside the envelopes is forbidden." 431 U.S. at 624. Indeed, there can be no customs-based rationale for reading the contents of cloud-based services, because individuals cannot be said to transport *across the border* digital data that is not stored on their device but merely accessible through the internet. The same is true for deleted data that can be retrieved during a forensic search. *Cf.* Br. of Appellee, *United States v. Vergara*, No. 16-15059, 2017 WL 360182, at *27 (11th

Cir. Jan. 23, 2017) (government argument in pending Eleventh Circuit case that border searches are justified because they "afford[] travelers *ample opportunity to limit the items that may be subjected to a search*" (emphasis added)).

And in cases involving forensic searches of device contents, "the immediate national security concerns [are] somewhat attenuated." *Kim*, 103 F. Supp. 3d at 56–57. Forensic searches occur days or weeks after the border crossing and can continue for long periods of time. *See, e.g.*, *Cotterman*, 709 F.3d at 967 ("[In a forensic search,] agents will mine every last piece of data on [travelers'] devices [and] deprive them of their most personal property for days (or perhaps weeks or even months, depending on how long the search takes)."); *Kim*, 103 F. Supp. 3d at 42 (quoting government agent's statement that the "identification and extraction process . . . may take weeks or months" (internal quotation marks omitted)). Though the government retains an interest in interdicting contraband and dangerous items, the imperative of conducting an immediate, warrantless search dissipates. There is ample time between initial seizure of a device and commencement of a forensic or forensic-like search to obtain a warrant from a judge. *Riley*, 134 S. Ct. at 2493 ("Recent technological advances similar to those discussed here have, in addition, made the process of obtaining a warrant itself more efficient."). In such cases, the search does "'not possess the characteristics of a border search or other regular inspection procedures'" but "'more resemble[s] the

common nonborder search based on individualized suspicion, which must be prefaced by the usual warrant and probable cause standards.'" *Kim*, 103 F. Supp. 3d at 58 (quoting *United States v. Brennan*, 538 F.2d 711, 716 (5th Cir. 1976)).

Obtaining a warrant before conducting a device search is fully practicable, and the aim of the border search doctrine—to detect contraband and determine admissibility—can be fully achieved while abiding by the warrant requirement. Requiring a warrant in the border context also prevents the government from conducting an end-run around *Riley*'s warrant requirement for searches of electronic devices inside the country, and around other statutory and constitutional protections against accessing the content of digital communications, a concern that is illustrated by the government's conduct in this case. *See, e.g.*, *Warshak*, 631 F.3d at 283 (discussing requirements of Stored Communications Act when accessing email content); *Molina-Isidoro*, 2016 WL 8138926, at *2 (describing government's search of Uber and WhatsApp applications on defendant's device *after* her arrest).

But even if this Court were to conclude that obtaining a warrant is not practicable, agents should still be required to have probable cause. *Cf. California v. Acevedo*, 500 U.S. 565, 579–80 (1991) (discussing automobile exception to warrant requirement, which requires officers to nonetheless have probable cause). A probable cause threshold will help limit the massive privacy intrusion inflicted

by device searches. *See Laich*, 2010 WL 259041, at *4. This will be particularly true as the search capabilities available to the government become more powerful and efficient. "It is little comfort to assume that the government—for now—does not have the time or resources to seize and search the millions of devices that accompany the millions of travelers who cross our borders. It is the potential unfettered dragnet effect that is troublesome." *Cotterman*, 709 F.3d at 966.

IV. At an Absolute Minimum, Searches of Electronic Devices Seized at the Border Require Reasonable Suspicion Because They Are Non-Routine.

Although the Supreme Court has held that the government has broad powers to conduct searches at the border, *see Ramsey*, 431 U.S. at 616, it has also recognized that non-routine border searches require at least reasonable suspicion of wrongdoing, *Montoya de Hernandez*, 473 U.S. at 541; *see also United States v. Kelly*, 302 F.3d 291, 294 (5th Cir. 2002). Furthermore, this Court has recognized that, in the border search context, "what constitutes 'reasonable suspicion' to justify a particular search may not suffice to justify a more intrusive or demeaning search." *United States v. Afanador*, 567 F.2d 1325, 1328 (5th Cir. 1978).

Searches of electronic devices are non-routine for a number of reasons. First, they are uniquely invasive, as the Supreme Court recognized in *Riley*. Such searches lay bare every bit of information in a person's device, becoming "essentially a computer strip search." *Cotterman*, 709 F.3d at 966; *cf. Montoya de Hernandez*, 473 U.S. at 541 n.4 (identifying strip searches as "nonroutine border

searches"). The comprehensive access to stored files, and in a forensic search to deleted data, metadata, and other hard-to-access digital information, means that a government agent can find out more information about a person than any other single search could likely reveal. Notably, the impracticability of deleting sensitive or hard-to-access content each time one travels, as well as the government's ability to access deleted files through forensic searches, makes it nearly impossible to effectively remove private information from electronic devices in the same way that one could leave a sensitive physical file at home prior to crossing the border. *Cf. Cotterman*, 709 F.3d at 965. Individuals' privacy and dignity interests in the contents of their electronic devices more closely resemble the heightened interests associated with private dwelling areas than luggage and other effects, and should be treated accordingly. *See United States v. Whitted*, 541 F.3d 480, 488 (2008) (search of passenger cabin of a vessel requires reasonable suspicion); *United States v. Alfonso*, 759 F.2d 728, 738 (9th Cir. 1985) (search of the private living quarters on a ship "should require something more than naked suspicion").

Second, forensic searches are often conducted at off-site facilities and are thus unbounded by time. A hallmark of routine border searches is that agents generally have to complete them within a reasonable amount of time, out of necessity given the large number of travelers crossing the border daily, and as a constitutional matter. *See Montoya de Hernandez*, 473 U.S. at 542–44. As the

length of time between the border crossing and the search increases, a higher level of suspicion becomes necessary. *See, e.g.*, *United States v. Yang*, 286 F.3d 940, 948 (7th Cir. 2002). Given the scope of information available on a phone, the duration of any search of the device is likely to exceed a typical luggage search, and forensic searches can occur at separate facilities where a traveler's electronic devices are reviewed for days or weeks, and where copies of those devices' hard drives are kept indefinitely.

Finally, reasonable suspicion is required because of the "particularly offensive manner" in which electronic device searches are carried out. *See Ramsey*, 431 U.S. at 618 n.13 (citing as an example for comparison *Kremen v. United States*, 353 U.S. 346, 347 (1957) ("The seizure of the entire contents of the house and its removal some two hundred miles away to the F.B.I. offices for the purpose of examination are beyond the sanction of any of our cases.")). Because device searches can indiscriminately lay bare the entire contents of a device without limits on the search's duration, subject matter, or scope, such searches are particularly "intrusive or demeaning," *see Afanador*, 567 F.2d at 1328. Thus, while searches of electronic devices at the border require a warrant or probable cause for the reasons described above, *see supra*, they also require at least reasonable suspicion as non-routine border searches.

CONCLUSION

This Court should hold that in this case, the post-arrest search of the defendant's electronic device required a warrant pursuant to the Supreme Court's clear directive in *Riley*. In the alternative, this Court should hold that because searches of electronic devices seized at the border infringe deeply on privacy interests, such searches should be permitted only pursuant to a warrant or, at a minimum, probable cause.

August 22, 2017

Respectfully submitted,

/s/ *Esha Bhandari*
Esha Bhandari
Nathan Freed Wessler
Vera Eidelman*
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ebhandari@aclu.org
**Admitted to the State Bar of California*

Paloma Wu**
ACLU of Mississippi Foundation
233 East Capitol Street
Jackson, MS 39201
Phone: 601-354-3408
Fax: 601-355-6465
pwu@aclu-ms.org

***Not yet admitted to Mississippi Bar*

Counsel for amici curiae

Edgar Saldivar
Texas Bar No. 24038188
ACLU Foundation of Texas
1500 McGowen St., Ste. 250
Houston, TX 77004
Phone: 713-942-8146
Fax: 713-942-8966
esaldivar@aclutx.org

Kali Cohn
Texas Bar. No. 24092265
ACLU Foundation of Texas
6440 N. Central Expressway
Dallas, TX 75206
Phone: 214-346-6577
Fax: 713-942-8966
kcohn@aclutx.org

Bruce Hamilton
ACLU Foundation of Louisiana
P.O. Box 56157
New Orleans, LA 70156
Phone: (504) 522-0628
Fax: (504) 613-6511
bhamilton@laaclu.org

CERTIFICATE OF COMPLIANCE

1. This brief complies with type-volume limits because, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f), it contains 6,491 words.

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman.

/s/ Esha Bhandari

Esha Bhandari

August 22, 2017

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 22nd day of August, 2017, the foregoing Brief of *Amici Curiae* American Civil Liberties Union, et al., was filed electronically through the Court's CM/ECF system. Notice of this filing will be sent by email to all parties by operation of the Court's electronic filing system.

/s/ Esha Bhandari

Esha Bhandari