No. 15-4111

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA

Plaintiff–Appellee,

v.

ALI SABOONCHI,

Defendant–Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND, SOUTHERN DIVISION

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION AND AMERICAN CIVIL LIBERTIES UNION OF MARYLAND IN SUPPORT OF DEFENDANT-APPELLANT

David R. Rocah
American Civil Liberties Union Foundation of Maryland
3600 Clipper Mill Road, Suite 350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
rocah@aclu-md.org

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTEREST OF AMICI CURIAE[1]

The American Civil Liberties Union ("ACLU") is a nationwide, non-profit, non-partisan public interest organization of more than 500,000 members dedicated to defending the civil liberties guaranteed by the Constitution. The ACLU of Maryland, the organization's affiliate in Maryland, was founded in 1931 to protect and advance civil rights and civil liberties in that state, and currently has approximately 14,000 members. The protection of privacy as guaranteed by the Fourth Amendment is of special concern to both organizations. The ACLU has been at the forefront of numerous state and federal cases addressing the right of privacy.

[1] Pursuant to Rule 29(a), counsel for *amici curiae* certifies that all parties have consented to the filing of this brief. Pursuant to Rule 29(c)(5), counsel for *amici curiae* states 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. Hundreds of millions of people cross the United States' borders every year,[2] traveling for business, pleasure, and family obligations. Large numbers of those travelers carry with them 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 stored on these devices can be deeply sensitive and private, including personal correspondence, family photos, medical records, intimate relationship details, proprietary business information, and more. Yet, despite the tremendous quantities of private data contained on these devices, the government claims the right to seize them at the border and subject them to even the most comprehensive and invasive forensic searches with no warrant or individualized suspicion whatsoever.

Given the significant privacy interests at stake, this Court should take the opportunity to clarify the Fourth Amendment standards governing such searches in order to provide guidance to the government and the traveling public. Because of

[2] *See* Lisa Seghetti, Cong. Research Serv., R43356, *Border Security: Immigration Inspections at Ports of Entry* 1 (2015), https://www.fas.org/sgp/crs/homesec/R43356.pdf ("About 362 million travelers (citizens and non-citizens) entered the United States in FY2013.").

the unique privacy concerns raised by forensic and forensic-like searches of portable electronic devices, this Court should hold that such searches may only be conducted pursuant to a warrant or, at an absolute minimum, upon a determination of probable cause or reasonable suspicion. This Court should so hold even if it determines that the government had the requisite level of suspicion in this particular case, because otherwise a "significant diminution of privacy" would result. *Id.* at 2493.

ARGUMENT

I. This Court Should Decide the Fourth Amendment Question Regardless of Whether Suppression is Warranted.

The district court in this case conducted a detailed analysis of the central Fourth Amendment question presented: what level of suspicion is required before the government may seize a person's smartphone, laptop, or other electronic device at the border and subject it to a forensic search. Recognizing the "difficult issues raised by a forensic search of digital devices seized at the border," JA 334, the court discussed its reasoning in depth before concluding that "a forensic search of an electronic device seized at the border cannot be performed absent reasonable, articulable suspicion." JA 349–50. Only then did it turn to assessing whether the government's forensic search of Mr. Saboonchi's electronic devices was in fact justified under that standard. JA 389. This Court should follow the same order of

analysis in order to provide guidance to the government and the public about the extent of Fourth Amendment protections for the extraordinarily voluminous and private information contained in the electronic devices we carry with us virtually wherever we go. In other words, even if this Court ultimately determines that the government had the appropriate quantum of suspicion to justify the forensic search of Mr. Saboonchi's electronic devices in this case, it should still decide the constitutional issue. Without guidance from this Court, a traveler "cannot know the scope of his constitutional protection, nor can a policeman know the scope of his authority." *New York v. Belton*, 453 U.S. 454, 459–60 (1981).

Every month, tens of millions of people travel through border crossings, international airports, and other ports of entry into the United States. U.S. Dep't of Homeland Sec., *Civil Rights/Civil Liberties Impact Assessment: Border Searches of Electronic Devices* 1 (Dec. 29, 2011)[3] ("DHS CR/CL Impact Assessment") (reporting monthly average of 29,357,163 travelers through all ports of entry in FY 2010); *see also United States v. Cotterman*, 709 F.3d 952, 956 (9th Cir. 2013) (en banc) ("Every day more than a million people cross American borders."). Hundreds of thousands of those travelers each month are directed by Customs and Border Protection agents to secondary screening, and hundreds of those have their portable electronic devices confiscated and searched. DHS CR/CL Impact

[3] http://www.dhs.gov/sites/default/files/publications/Redacted%20Report.pdf.

Assessment 1; *see also* American Civil Liberties Union, *Government Data About Searches of International Travelers' Laptops and Personal Electronic Devices*[4] (analysis of government documents released under Freedom of Information Act finding that "[b]etween October 2008 and June 2010, over 6,500 people traveling to and from the United States had their electronic devices searched at the border. Nearly half of these people were U.S. citizens."). While some devices are searched contemporaneously at the border by agents and then returned to travelers before they go on their way, other devices are held for weeks or months and subjected to exhaustive forensic search techniques. Yet, despite the incidence and invasiveness of these forensic searches, only one court of appeals has yet addressed the Fourth Amendment standard governing such searches. *See Cotterman*, 709 F.3d at 957. Because forensic (and other similarly invasive) searches of people's electronic devices impinge deeply on vital privacy interests, and because this Court is unlikely to be presented with other avenues for answering the question presented, the Court should issue a reasoned opinion providing the proper standard upon which the government may forensically search an electronic device seized at the border.

[4] https://www.aclu.org/government-data-about-searches-international-travelers-laptops-and-personal-electronic-devices.

A. Forensic and Forensic-Like Searches of Travelers' Electronic Devices Pose Serious Privacy Concerns.

As a matter of longstanding policy and practice, the U.S. Government claims the authority to search international travelers' electronic devices without any particularized or individualized suspicion, let alone a search warrant or probable cause. Both U.S. Customs and Border Protection ("CBP") and U.S. Immigration and Customs Enforcement ("ICE") have formal written policies permitting border officials to read and analyze information on international travelers' electronic devices without a warrant or individualized suspicion. CBP, "Border Search of Electronic Devices Containing Information," Directive No. 3340-049, § 5.1.2 (Aug. 20, 2009)[5] ("CBP Policy"); ICE, "Border Searches of Electronic Devices," Directive No. 7-6.1, § 6.1 (Aug. 18, 2009)[6] ("ICE Policy"). Both agencies' policies permit border officials to read and analyze—without individualized suspicion—even legal or privileged information, information carried by journalists, medical information, confidential business information, and other sensitive information. The ICE policy states unequivocally 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). CBP policy states that "legal materials" "may be subject" to

[5] *Available at* http://www.dhs.gov/sites/default/files/publications/cbp_directive_3340-049%20Homeland%20directive_0.pdf.

[6] *Available at* http://www.dhs.gov/sites/default/files/publications/7-6.1%20directive.pdf.

the requirement that an agent "seek advice" from counsel, but does not require agents to seek such advice. CBP Policy § 5.2.1.

These policies remain in effect, and have been reaffirmed in recent years, both in policy documents, *see, e.g.*, DHS CR/CL Impact Assessment 3 ("[W]e are not recommending that officers demonstrate reasonable suspicion for the device search . . . ."), and in litigation filings.[7] The effect of these policies is significant, both because of the number of travelers crossing U.S. borders, and because of the volume and variety of sensitive information contained on electronic devices in their possession.[8]

Use of mobile computing devices is pervasive. More than 90% of American adults own a cell phone of some kind, *Riley*, 134 S. Ct. at 2490, and 64% of American adults own a smartphone, with rates of smartphone ownership even

---

[7] *See, e.g.*, JA 97–99; *see also, e.g.*, Gov't's Opp'n to Def.'s Mot. To Suppress Evidence at 6, *United States v. Kim*, No. 13-0100, 2015 WL 2148070 (D.D.C. May 8, 2015), ECF No. 37 (3/18/15) ("The search of defendant Kim's laptop was conducted pursuant to the border search authority outlined above, and thus did not require any level of suspicion or a search warrant.").

[8] The government's claimed authority to conduct suspicionless forensic searches of electronic devices seized at the border applies not only to travelers entering the country, but to those departing it as well. *See* CBP Policy § 1 (policy applies to searching electronic devices "encountered by U.S. Customs and Border Protection (CBP) at the border, both inbound and outbound"); ICE Policy § 1.1 ("This Directive applies to searches of electronic devices of all persons arriving in, departing from, or transiting through the United States."); *see also, e.g.*, *Kim*, 2015 WL 2148070, at *5 (seizure of laptop from traveler boarding international flight from Los Angeles International Airport).

higher "among younger Americans, as well as those with relatively high income and education levels,"[9] which happen also to be groups that travel internationally at particularly high rates.[10] Other types of mobile electronic devices also have high rates of use, with 42% of American adults owning a tablet computer and 32% owning an e-reader.[11] More than 80% of U.S. households have a laptop computer.[12]

People consistently carry these devices with them, including when they travel. Indeed, "[a]ccording to one poll, nearly three-quarters of smart phone users

---

[9] Aaron Smith, Pew Research Ctr., *U.S. Smartphone Use in 2015* (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

[10] As of 2014, the median household income of international travelers from the United States was $100,000. U.S. Dep't of Commerce, Nat'l Travel & Tourism Office, *Profile of U.S. Resident Travelers Visiting Overseas Destinations: 2014 Outbound* 14, *available at* http://travel.trade.gov/outreachpages/download_data_table/2014_Outbound_Profile.pdf. The median household income in the United States generally as of 2013 was approximately half that: $51,939. U.S. Dep't of Commerce, U.S. Census Bureau, *Income & Poverty in the United States: 2013*, at 5 (Sept. 2014), *available at* http://www.census.gov/content/dam/Census/library/publications/2014/demo/p60-249.pdf. International travel by younger travelers is increasing at a rate greater than other travelers. 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/.

[11] Pew Research Center, *Mobile Technology Fact Sheet*, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.

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

report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." *Riley*, 134 S. Ct. at 2490. As the district court explained, mobile devices are no longer merely a convenience for travelers, but are often a necessity, serving "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 and, particularly, of traveling to unstable or dangerous regions of the world." JA 366. People increasingly rely on their electronic devices for communication (via text messages, calls, email, and social networking), navigation, entertainment, news, photography, videography, and a multitude of other functions,[13] and it is no wonder that they use their devices for these purposes while traveling outside the country just as when remaining within it. Moreover, a person who travels with one electronic device will often travel with several, thus multiplying the digital data in their possession. *See, e.g.*, *United States v. Hassanshahi*, 75 F. Supp. 3d 101, 106–07 (D.D.C. 2014) (discussing seizure of international traveler's "laptop computer, multimedia cards, thumb drives, a camcorder, SIM cards, and a cell phone").

[13] *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 (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/chapter-three-a-week-in-the-life-analysis-of-smartphone-users/.

When a traveler's electronic device is seized and 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) ("[E]ven inexpensive electronic storage media today can store the equivalent of millions of pages of information."); *Cotterman*, 709 F.3d at 964. Today's hard drives are even more capacious. Laptops sold in 2015 can have storage capacities ranging up to one terabyte or more,[14] the equivalent of more than 600 million pages of text. *See* LexisNexis, *How Many*

[14] *See* Mark Kyrnin, *Guide To Laptop Storage Devices*, About Tech, http://compreviews.about.com/od/storage/a/Laptop-Drive-Buyers-Guide.htm; Apple, *Compare Mac Models*, https://www.apple.com/mac/compare/ (last accessed Sept. 9, 2015); JA 374 n.15.

Pages in a Gigabyte (2007).[15] Even tablet computers can be purchased with 512 gigabytes of storage.[16]

Smaller computing devices, including smartphones and USB flash drives, can also hold phenomenal quantities of data. As the district court explained, the eight-gigabyte USB drive seized from Mr. Saboonchi "could hold the equivalent of thirty-two suitcases" worth of printed pages. JA 374. That is a small storage capacity by today's standards, with USB drive capacity reaching 256 gigabytes[17] and portable external hard drive capacity up to three or four terabytes.[18] Smartphones also provide large storage capacities. "The iPhone 4s that Saboonchi was carrying is available with a storage capacity ranging from eight to sixty-four gigabytes," JA 374 n.15 (citation omitted), and the latest iPhone model comes with up to 128 gigabytes of storage capacity.[19] Even older smartphones with smaller

---

[15] http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf. The entire printed collection of the U.S. Library of Congress is estimated to comprise ten terabytes of data. *See Data Powers of Ten*, in *How Much Information?* (2000), http://www2.sims.berkeley.edu/research/projects/how-much-info/datapowers.html.

[16] *See* Microsoft, *Surface Pro 3*, https://www.microsoft.com/surface/en-us/products/surface-pro-3 (last accessed Sept. 9, 2015).

[17] *See, e.g.*, PNY, *USB Flash Drives*, https://www.pny.com/mega-consumer/shop-all-products/usb-flash-drives (last accessed Sept. 9, 2015).

[18] *See, e.g.*, Western Digital, *External Portable Hard Drives*, http://www.wdc.com/en/products/external/portable/ (last accessed Sept. 9, 2015).

[19] Apple, *Identify Your IPhone Model*, https://support.apple.com/en-us/HT201296 (last accessed Sept. 9, 2015).

storage capacities can hold the equivalent of "millions of pages of text, thousands of pictures, or hundreds of videos." *Riley*, 134 S. Ct. at 2489. And because "computer storage capabilities tend to double about every two years," the amount of data easily carried on a laptop computer, smartphone, or other portable electronic device will continue to increase at a rapid clip. *Kerr*, 199 Harv. L. Rev. at 542. Moreover, the availability of cloud-based storage services can exponentially increase the functional capacity of a device.[20]

Not only can these portable devices contain great quantities of data, but they also contain a diverse array of information, much of it exceedingly sensitive. As the Supreme Court explained last year, smartphones are "minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Riley*, 134 S. Ct. at 2489; *see also Cotterman*, 709 F.3d at 964 ("Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: 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

[20] *See, e.g.*, Google, *Drive Help*, https://support.google.com/drive/answer/2375123 (offering 15 gigabytes of free cloud storage and up to 30 terabytes of paid cloud storage).

people's mobile devices, including internet browsing history,[21] medical records,[22] historical cell phone location data,[23] email,[24] privileged communications,[25] and information about First Amendment–protected association.[26]

---

[21] *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."); *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

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

[23] *See Riley*, 134 S. Ct. at 2490 ("Data on a cell phone can also reveal where a person has been. 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."); *United States v. Graham*, __ F.3d __, 2015 WL 4637931, at *12 (4th Cir. Aug. 5, 2015) ("[T]he government invades a reasonable expectation of privacy when it relies upon technology not in general use to discover the movements of an individual over an extended period of time.").

[24] *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.").

[25] *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).

[26] *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 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 as effective a restraint on freedom of association . . . .").

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 2490. Much of the private data that can be excavated 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. JA 375–84; *Cotterman*, 709 F.3d at 965; *Riley*, 134 S. Ct. at 2490–91.

As the Supreme Court explained in *Riley*, any search of a mobile device implicates serious privacy interests. *Riley*, 134 S. Ct. at 2488–89. But forensic searches, as well as other kinds of similarly exhaustive searches, can be significantly more invasive than more conventional searches carried out by an agent manually clicking through a device. This is not to say that the more conventional searches do not impinge deeply on privacy interests. They do. But because only forensic searches are at issue in this case, *see* JA 339, this Court need not address what standard should apply to other types of device searches at the

border. Forensic and forensic-like searches clearly cross the threshold requiring heightened Fourth Amendment protection.

A forensic search begins with an agent making a mirror-image copy of the device's entire hard drive or other digital storage repository, including all active files, deleted files,[27] allocated and unallocated file space,[28] metadata, and password-protected or encrypted data. Nat'l Inst. of Justice, U.S. Dep't of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* 16 (Apr. 2004)[29]; Kerr, 119 Harv. L. Rev. at 540. That copy is then analyzed using powerful forensic search 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. JA 380–81 (discussing access to deleted files); *see also* JA 65 ("This examiner recovered the contacts, call logs, calendar entries, text messages, email, chat logs, WiFi connection information, web browser information, photos, and video files [from the smartphone].").

[27] "[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.

[28] "'Unallocated space is space on a hard drive that contains deleted data, usually emptied from the operating system's trash or recycle bin folder, 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).

[29] *Available at* https://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

The forensic search tools used by the government can extract and analyze tremendous quantities of data.[30] In one recent case, for example, an agent "employed a software program called EnCase . . . . to export six Microsoft Outlook email containers[, which 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. *Kim*, 2015 WL 2148070, at *6–7 & n.3 (footnote omitted). He then "used another program, Intella, to process the files," including to "index and categorize" the "thousands of emails" on the device, a task that would have been "impractical" without the specialized forensic software. *Id.* at *6–7 (citations and internal quotation marks omitted). Because of these capabilities, "[a]n exhaustive forensic search of a copied laptop hard drive intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border." *Cotterman*, 709 F.3d at 966.

[30] Forensic searches are not the only way the government can uncover large quantities of sensitive data from an electronic device. *See Kim*, 2015 WL 2148070, at *19 ("[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 and use that 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 ("For those hard to find files, Recuva has an advanced deep scan mode that scours your drives to find any traces of files you have deleted.").

Forensic-type searches have the capability to be significantly more invasive than other searches, both because they read and analyze the entirety of the vast amount of data stored on a mobile device at the push of a button, and because they search and analyze data (like deleted files) that a human, unassisted by specialized tools, could not have accessed. *See generally*, *Cotterman*, 709 F.3d at 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. Jones*, 132 S. Ct. 945. Because the privacy invasion is so acute, the need for judicial guidance is pressing.

B. This Court Is Unlikely To Be Presented With Other Opportunities To Resolve the Question Presented, and Should Take the Opportunity to Do So Now.

The serious threat to privacy posed by warrantless, suspicionless forensic searches of travelers' mobile electronic devices requires authoritative resolution by this Court. This Court should decide what level of suspicion the Fourth Amendment requires for such searches before addressing whether the government actually had that quantum of suspicion in this case. That was the path taken by the Ninth Circuit in *Cotterman* and by the district court below, and it is the right course here. *See Cotterman*, 709 F.3d at 968; JA 386–89. Without an explanation of how the Fourth Amendment applies to these searches, the protections of the Constitution risk becoming dead letter for the millions of Americans who cross our

nation's borders each year, including the millions who enter and leave the country through international airports and seaports in this Circuit.[31]

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 Warshak*, 631 F.3d at 285 ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."). As this Court recently explained, "[o]ur review of well settled Fourth Amendment jurisprudence teaches us that, even as technology evolves, protections against government intrusion should remain consistent with those privacy expectations society deems reasonable." *Graham*, 2015 WL 4637931, at *19. Ensuring a consistent level of protection requires courts to rule on Fourth Amendment questions like the one in this case when presented to them. To paraphrase the Sixth Circuit, "[i]f every court confronted with a novel Fourth Amendment question were to skip directly to [invocation of avoidance doctrines], the government would be given *carte blanche*

[31] *See, e.g.*, U.S. CBP, *Washington Dulles International Airport (IAD)*, http://www.cbp.gov/travel/international-visitors/travel-tourism/washington-dulles-international-airport-iad ("From Fiscal Year (FY) 2009-2013, IAD experienced an approximate 13% increase in international traveler arrivals (3.05 million to 3.46 million)."); U.S. Dep't of Transp., Maritime Admin., *North American Cruise Statistical Snapshot, 2011*, at 8 (Mar. 2012), http://www.marad.dot.gov/wp-content/uploads/pdf/North_American_Cruise_Statistics_Quarterly_Snapshot.pdf (showing 254,000 cruise passengers departing from Baltimore and 165,000 from Charleston in 2011).

to violate constitutionally protected privacy rights" in future investigations. *Warshak*, 631 F.3d at 282 n.13.

The need to resolve the standard governing invasive searches of mobile devices seized at the border is particularly pressing because the question is unlikely to arise in civil challenges brought to vindicate the rights of undisputedly innocent persons. Even when a person's mobile devices have been seized and forensically searched, courts may dismiss declaratory and injunctive claims on standing grounds, on the theory that the likelihood of renewed injury from possible future seizures and searches of electronics at the border is not sufficiently concrete. *See Abidor v. Napolitano*, 990 F. Supp. 2d 260, 270–77 (E.D.N.Y. 2013) (dismissing declaratory and injunctive relief claims challenging suspicionless forensic border search of laptop on standing grounds). Further, in the absence of appellate precedent in this Circuit, damages claims for suspicionless electronic-device searches may be derailed by the doctrine of qualified immunity. *See Pearson v. Callahan*, 555 U.S. 223, 236 (2009) (holding that courts may grant qualified immunity without deciding first whether there was an underlying constitutional violation). Perhaps reflecting these barriers to review, only one court of appeals has yet addressed the important question of constitutional interpretation raised in this case. *Cotterman*, 709 F.3d at 952. And that court did so before the Supreme Court decided *Riley v. California*, which counsels adoption of a more privacy-

protective rule than the *Cotterman* court contemplated. This Court should take up the mantle of ensuring that the Fourth Amendment is not allowed to ossify 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 do not apply to the question presented here. The government claims that *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005), justifies the suspicionless forensic search of the defendant's mobile electronic devices. JA 97. *Ickes* involved a search of electronic devices at the border that was not nearly as exhaustive as the forensic copying and search at issue here. The defendant's only argument in *Ickes* was about the need for a heightened Fourth Amendment standard when "expressive materials" are searched. *Ickes*, 393 F.3d at 506. The acute privacy harm of forensic searches of digital media was not at issue, and this Court should make clear that neither the facts nor reasoning of *Ickes* justify the extraordinarily invasive searches that occurred in this case.[32]

[32] Because this case involves a forensic search—and exclusively a forensic search, *see* JA 339—of Mr. Saboonchi's electronic devices, this Court need not address whether the holding of *Ickes*, as it applies to more conventional searches, is still good law in light of *Riley*.

II. Forensic or Forensic-Like Search of Electronic Devices Seized at the Border Requires 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,[33] search pursuant to exigent circumstances,[34] vehicular search,[35] and border search.[36] None of these exceptions automatically apply merely upon their invocation, however, but rather 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, although the border-search exception to the warrant requirement is broad, it does not cover the highly invasive

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

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

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

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

forensic search of smartphones, laptops, and other mobile electronic devices. "[A]ny extension of that reasoning to digital data has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489.

Like other exceptions to the warrant requirement, the border-search doctrine relies on a balancing of the government's relevant interests against the individual's privacy interest. *See United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985); *Riley*, 134 S. Ct. at 2484; *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999). Because "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border," *Flores-Montano*, 541 U.S. at 152, the balance is generally "struck much more favorably to the Government" in the border-search context. *Montoya de Hernandez*, 473 U.S. at 540. "Even at the border," however, "individual privacy rights are not abandoned." *Cotterman*, 709 F.3d at 960.

In *Riley*, the Supreme Court engaged in a balancing of interests in an analogous context,[37] concluding 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

[37] The Supreme Court has noted that the border-search and search-incident-to-arrest exceptions are rooted in the same values: "[T]he '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 . . . ." *United States v. Ramsey*, 431 U.S. 606, 621 (1977) (citation omitted).

S. Ct. at 2484–85. The *Riley* opinion "demonstrate[s] how th[e balancing] analysis is supposed to proceed" and "strongly indicate[s] that a digital data storage device cannot fairly be compared to an ordinary container when evaluating the privacy concerns involved," even in the border-search context. *Kim*, 2015 WL 2148070, at *18–19.

Riley's holding provides guideposts for deciding this case, and counsels that a warrant should be required. On one side of the balance, the individual privacy interest in the contents of a cell phone or laptop is extraordinarily strong. *E.g.*, *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."); *supra* Part I.A. The privacy harms inflicted by forensic and forensic-like searches are particularly acute, surpassing even what the *Riley* Court contemplated. *Supra* Part I.A; JA 377 ("[A] forensic search is a different *search*—not merely a search of a different object—and it fundamentally alters the playing field for all involved."). This is so in part because of the unrivaled comprehensiveness of the search and the volume and diversity of private information affected.

It is also so because of the duration of the interference with an individual's Fourth Amendment rights. *Cf. United States v. Place*, 462 U.S. 696, 699, 708-10 (1983) (length of detention of a traveler's luggage is an "important factor" in determining what level of suspicion is required). By copying the entire contents of

a device and holding 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 for which a warrant is required, and as long as the government retains the copy, the intrusion on Fourth Amendment interests continues. *See United States v. Ganias*, 755 F.3d 125, 137 (2d Cir. 2014) ("[Copying the contents of a computer] enabled the Government to possess indefinitely personal records . . . . This was a meaningful interference with [the defendant's] possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment."), *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015). 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).

On the other side of the balance, in cases like this one involving forensic searches, "the immediate national security concerns [are] somewhat attenuated." *Kim*, 2015 WL 2148070, at *20. 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*, 2015 WL 2148070, at *8 (quoting Department of Homeland Security Agent's statement that "[t]he identification and extraction process . . . may take weeks or months."). Though the government retains an interest in interdicting contraband and ensuring border security during that time, 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."). The search in this case "'did not possess the characteristics of a border search or other regular inspection procedures. It more resembled the common nonborder search based on individualized suspicion, which must be prefaced by the usual warrant and probable cause standards.'" *Kim*, 2015 WL 2148070, at *21 (quoting *United States v. Brennan*, 538 F.2d 711, 716 (5th Cir. 1976)).

Requiring a warrant also prevents the government from conducting an end-run around the warrant requirement imposed by *Riley* for searches of electronic devices inside the country. In this case, the government had long suspected Mr. Saboonchi of violating the law. JA 226–27. Assuming the government had

probable cause, it could have gone to a judge, obtained a warrant, and served it on Mr. Saboonchi at his home in Maryland. Instead, the government lay in wait for Mr. Saboonchi to exit and reenter the country, which he fortuitously happened to do for a one-day sightseeing trip with his wife. JA 191. Had the government acted in the normal course, it would have needed a warrant. It should not be able to side-step that requirement as it attempted to do here.

Obtaining a warrant before conducting a forensic search is fully practicable, and the aim of the border search doctrine—to detect contraband and threats—can be fully achieved while abiding by the warrant requirement. But even if this Court were to conclude that obtaining a warrant is not practicable or is inconsistent with the need to secure the border, 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 have probable cause even in the absence of a warrant). A probable-cause threshold will ensure that the massive privacy intrusion inflicted by forensic and forensic-like searches is restricted to only those cases where it is truly justified. *Laich*, 2010 WL 259041, at *4. This will be particularly true as the forensic search technology deployed by the government becomes 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 for unfettered dragnet effect that is troublesome." *Cotterman*, 709 F.3d at 966.

III. At an Absolute Minimum, Forensic and Forensic-Like Searches of Electronic Devices Seized at the Border Require Reasonable Suspicion.

Although the Supreme Court has found 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. Oriakhi*, 57 F.3d 1290, 1297 (4th Cir. 1995). When deciding whether a search is non-routine, "[t]he determining factor is . . . 'the level of intrusion into a person's privacy.'" *Tabbaa v. Chertoff*, 509 F.3d 89, 98 (2d Cir. 2007) (citation omitted); *accord United States v. Braks*, 842 F.2d 509, 511 (1st Cir. 1988) (determining factor in assessing whether a search is non-routine is "[t]he degree of invasiveness or intrusiveness."); *United States v. Vega–Barvo*, 729 F.2d 1341, 1346, 1349 (11th Cir. 1984) (searches are deemed non-routine based on the amount of "personal indignity" they cause and their "intrusive[ness]").

Forensic-type searches of electronic devices are non-routine for a number of reasons. First, forensic and forensic-like searches are uniquely invasive. By laying bare every bit of information in a person's device, the government conducts "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 saved files, deleted data, metadata, and other digital information means that a forensic examiner can find out more information about a person than any other single search could likely reveal.[38] *See* JA 383 ("Rather than a search of a suitcase, this would be as if, by opening a suitcase, a Customs officer could determine everywhere the suitcase had been taken, everything that had been packed within it, when and how it was acquired, and when each item last had been worn."). Notably, the capability to access deleted files makes it is nearly impossible to effectively remove private information from electronic devices in the same way that one could leave a sensitive file at home or take it out of a briefcase prior to crossing the border. *See 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. *Cf. United States v. Whitted*, 541 F.3d 480, 488 (3d Cir. 2008) (requiring reasonable suspicion for search of passenger cabin of a vessel); *United States v. Alfonso*, 759 F.2d 728, 738 (9th Cir. 1985) (finding that a border search of the

[38] This factor alone distinguishes this case from *Ickes*, in which the Court stated that "[c]ustoms agents have neither the time nor the resources to search the contents of every computer." 393 F.3d at 507. With forensic search technology, agents are gaining such ability, calling for a higher standard of suspicion than for conventional searches of electronics.

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 normal border searches is that agents generally have to complete them within a reasonable amount of time, both out of necessity given the large numbers of travelers crossing the border daily, and as a matter of constitutional law. *See Montoya de Hernandez*, 473 U.S. at 542–44. Forensic searches, however, necessarily occur at separate facilities where a traveler's electronic devices are reviewed for days or weeks, and where copies of those device's hard drives are kept indefinitely. As the duration of a border search lengthens, a higher level of suspicion becomes necessary. *See, e.g.*, *United States v. Yang*, 286 F.3d 940, 948 (7th Cir. 2002).

Finally, reasonable suspicion is required because of the particularly offensive manner in which forensic electronic device searches are carried out. In *Ramsey*, the Supreme Court stated that a border search may be constitutionally objectionable if it is carried out in a "particularly offensive manner." 431 U.S. at 618 n.13. By way of example, the Court identified cases involving wildly overbroad searches and seizures, suggesting that the execution of such searches is considered particularly offensive under the Constitution. *Id.* (citing *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.") and *Go–Bart Importing Co. v. United States*, 282 U.S. 344, 358 (1931) (concerning "unlimited search, ransacking the desk, safe, filing cases and other parts of [an] office" without a warrant)). Because forensic searches indiscriminately seize and analyze the entire contents of an electronic device, without limits on the search's duration, subject matter, or scope, such searches are particularly offensive. As described above, *supra* Part I.A, electronic devices contain vast quantities of deeply personal and sensitive information. A forensic or forensic-like search will reveal every nude photograph, every intimate email with a person's spouse or partner, every web search looking up symptoms of an embarrassing disease. Limiting searches to where the government can at least meet the reasonable suspicion standard will help reconcile the privacy interests of travelers with the government's need to enforce the law at the border. *See Cotterman*, 709 F.3d at 963–64.

CONCLUSION

This Court should hold that because forensic and forensic-like searches of smartphones, laptops, and other mobile electronic devices seized at the border infringe deeply on privacy interests, such searches should only be permitted

pursuant to a warrant, or at a minimum upon a determination of probable cause or reasonable suspicion.

September 10, 2015

Respectfully submitted,

/s/ Nathan Freed Wessler

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

David R. Rocah
American Civil Liberties Union Foundation of Maryland
3600 Clipper Mill Road, Suite 350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
rocah@aclu-md.org

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a) because it contains 6,998 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).

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/ Nathan Freed Wessler

Nathan Freed Wessler

September 10, 2015

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 10th day of September, 2015, the foregoing Amici Curiae Brief for the American Civil Liberties Union and American Civil Liberties Union of Maryland was filed electronically through the Court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system.

/s/ Nathan Freed Wessler

Nathan Freed Wessler