Case No. 15-4111

---

**IN THE UNITED STATES COURT OF APPEALS**
**FOR THE FOURTH CIRCUIT**

---

UNITED STATES OF AMERICA,

*Plaintiff-Appellee,*

v.

ALI SABOONCHI,

*Defendant-Appellant.*

---

# BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF APPELLANT

---

On Appeal from the United States District Court
for the District of Maryland
The Honorable Paul W. Grimm, U.S. District Court Judge
Case No. 8:13-cr-00100-PWG-1

---

Sophia Cope
Hanni Fakhoury
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, California 94109
Telephone: (415) 436-9333
Email: sophia@eff.org

*Counsel for Amicus Curiae*
ELECTRONIC FRONTIER
FOUNDATION

## DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amicus curiae* Electronic Frontier Foundation states that it does not have a parent corporation, and that no publicly held corporation owns 10% or more of the stock of *amicus*.

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

## Federal Cases

**Federal Statutes**



**Constitutional Provisions**



**Other Authorities**

## STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a San Francisco-based, non-profit, member-supported civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges industry, government, and the courts to support free expression, privacy, and openness in the information society. Founded in 1990, EFF has nearly 23,000 dues-paying members from across the United States. As a recognized expert focusing on the intersection of civil liberties and technology, EFF is particularly concerned with protecting digital privacy at a time when technological advances have resulted in an increased ability of the government to pry into the private lives of innocent Americans.[2]

[1] No party's counsel authored this brief in whole or in part. Neither any party nor any party's counsel contributed money that was intended to fund preparing or submitting this brief. No person other than *amicus*, its members, or its counsel contributed money that was intended to fund preparing or submitting this brief. All parties have consented to the filing of this brief.

[2] All webpages were last visited September 8, 2015.

## INTRODUCTION

Until the 21st century, the border search exception to the Fourth Amendment's warrant requirement was limited to the items travelers could carry with them when crossing the international border. The "amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile." *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (en banc). Because of this practical reality, citizens could take comfort that border searches did not give government access to travelers' entire homes or offices—indeed, their whole lives—in the absence of the Fourth Amendment's warrant requirement.

Today, the "sum of an individual's private life" sits in the pocket or purse of almost any traveller carrying a cell phone, laptop or tablet computer. *Riley v. California*, 134 S. Ct. 2473, 2489 (2014). The Supreme Court noted that cell phones in particular have become "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Id.* at 2484. As a result, *Riley* concluded that the ubiquity of cell phones—and other forms of modern mobile technology—combined with their capacity to hold vast quantities of different types of highly personal information makes them quantitatively and qualitatively different from their analog and physical counterparts. *Id.* at 2489.

*Riley* excluded the data on a cell phone from the category of things police can search without a warrant under the search-incident-to-arrest exception, instead requiring that police obtain a warrant based on probable cause. *Id.* at 2495. The Court reached this conclusion by finding that digital devices like cell phones are fundamentally different from physical containers, and because the purpose of searching digital devices incident to arrest is largely beyond the scope of the narrow rationales underlying this exception to the warrant requirement.

This Court should reach the same conclusion when it comes to the border search exception and require that the government obtain a probable cause warrant to search digital devices at the border.

Although the district court recognized the significant privacy interests in digital devices, it created an unworkable rule that fails to adequately protect the sensitive information stored on digital devices, and will lead to confusion for border agents and other courts. Instead of focusing on the highly personal nature of digital information, the district court focused on how that information is searched. Adopting the Ninth Circuit's dichotomy from *Cotterman*, the district court held that "forensic" searches of digital devices at the border require reasonable suspicion, while border agents may conduct "conventional" or "routine" searches without a warrant or any individualized suspicion pursuant to the border search exception. *United States v. Saboonchi*, 990 F. Supp. 2d 536, 547-49 (D. Md. 2014)

("*Saboonchi I*"); *United States v. Saboonchi*, 48 F. Supp. 3d 815, 819 (D. Md. 2014) ("*Saboonchi II*"); *see also Cotterman*, 709 F.3d at 966 (distinguishing "cursory" searches and "exhaustive forensic searches" of digital devices). This rule fails for two reasons.

First, any search of the data on a digital device is a "highly intrusive" search that implicates the "dignity and privacy interests" of the traveler, *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004), which should require a probable cause warrant based on the Supreme Court's clear guidance in *Riley*. This is especially true as digital devices permeate society and store increasing amounts of highly personal information. Additionally, as law enforcement tools advance—including devices that allow agencies to copy and search the entire contents of a smartphone in mere minutes—it is increasingly difficult to distinguish "conventional"/"routine" from "forensic" searches. Constitutional rights should not turn on such a flimsy distinction.

Second, if the "primary purpose" or "immediate objective" of a warrantless and suspicionless search would be "to generate evidence *for law enforcement purposes*," then the border search exception does not apply. *Ferguson v. City of Charleston*, 532 U.S. 67, 81-83 (2001) (emphasis in original). In the case of digital devices at the border, the primary purpose of data searches is almost always

ordinary criminal law enforcement, which falls outside the narrow purposes of the border search exception: immigration and customs enforcement.

Left undisturbed, the district court's approach would authorize law enforcement to use the border search exception as a pretext to search for evidence of any criminal activity without a warrant and often without any individualized suspicion whenever someone appears at the border. This would impermissibly "untether" such searches from the narrow justifications for the border search exception. *See Riley*, 134 S. Ct. at 2485.

A "person's digital life ought not to be hijacked simply by crossing a border." *Cotterman*, 709 F.3d at 965. *Amicus* urges this Court to require a warrant based on probable cause before the government may search the data on digital devices at the border.

## ARGUMENT

### I. Digital Devices Contain Vast Amounts of Highly Personal Information.

Before digital devices came along, border searches of personal property, like searches incident to arrest, were "limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy." *Riley*, 134 S. Ct. at 2489. In *Riley*, the government argued that the search of cell phone data is the same as searching physical items. *Id.* at 2488. The Court rejected this argument: "That is like saying a ride on horseback is materially indistinguishable from a

flight to the moon." *Id.* Instead, the Court looked to the nature of cell phones themselves—rather than how the devices are searched—to conclude that any search would implicate significant privacy interests. The Court stated that digital devices like "cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" *Riley*, 134 S. Ct. at 2494-95 (citing *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

The privacy interests in digital devices are even starker given the vast numbers of people who own them. Globally, 7.1 billion people own a cell phone, with 2.6 billion owning a smartphone.[3] Ninety percent of American adults own a cell phone, with 64 percent owing a smartphone.[4] Additionally, 32 percent of American adults own an e-reader and 42 percent own a tablet computer.[5] As the Supreme Court stated, "Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception." *Riley*, 134 S. Ct. at 2490.

---

[3] *Ericsson Mobility Report*, 2 (June 2015), http://www.ericsson.com/res/docs/2015/ericsson-mobility-report-june-2015.pdf.
[4] Pew Research Center, *Mobile Technology Fact Sheet*, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.
[5] *Id.*

Digital devices are both quantitatively and qualitatively different from physical containers. *Id.* at 2489; *see also United States v. Kim*, 2015 WL 2148070, *19 (D.D.C. May 8, 2015) (stating *Riley* "strongly indicate[d] that a digital data storage device cannot fairly be compared to an ordinary container when evaluating the privacy concerns involved"). Quantitatively, the vast amount of personal data on digital devices at the border is the same as if "a person's suitcase could reveal not only what the bag contained on the current trip, but everything it had ever carried." *Cotterman*, 709 F.3d at 965. The district court acknowledged "that the sheer quantity of information available on a cell phone makes it unlike other objects to be searched." *Saboonchi II*, 48 F. Supp. 3d at 819. With their "immense storage capacity," smartphones, laptops, tablets and other digital devices can contain the equivalent of "millions of pages of text, thousands of pictures, or hundreds of videos." *Riley*, 134 S. Ct. at 2489; *see also Cotterman*, 709 F.3d at 964 ("The average 400-gigabyte laptop hard drive can store over 200 million pages—the equivalent of five floors of a typical academic library.").[6]

Qualitatively, digital devices "collect[] in one place many distinct types of information … that reveal much more in combination than any isolated record."

[6] In this case, government agents searched Mr. Saboonchi's two smartphones and one flash drive. *Saboonchi I*, 990 F. Supp. 2d at 539. The district court calculated that "the eight-gigabyte USB drive that Saboonchi was carrying could hold the equivalent of thirty-two suitcases based on its size and, at 5,200 pounds, would exceed the weight limit for one hundred checked suitcases," which "strains analogies between computers and other closed containers." *Id.* at 561-62.

*Riley*, 134 S. Ct. at 2489. They "are simultaneously offices and personal diaries" and "contain the most intimate details of our lives." *Cotterman*, 709 F.3d at 964. Even the most basic digital devices hold a variety of information including "photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on." *Riley*, 134 S. Ct. at 2489. "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." *Id.* at 2490 (citing *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.")); s*ee also United States v. Graham*, 2015 WL 4637931, *11 (4th Cir. 2015). Thus, today's digital devices enable the reconstruction of "the sum of an individual's private life" covering a lengthy amount of time—"back to the purchase of the [device], or even earlier." *Id.* at 2489.

Even digital devices with more limited features and storage capacity than cell phones and computers contain vast amounts of highly personal information. Wearable fitness devices track a variety of data related to an individual's health.[7]

[7] *See*, *e.g.*, FitBit's Surge, which records steps, distance, floors climbed, calories burned, active minutes, workouts and sports played, sleep and heart rate; non-

E-readers can reveal every book a person has read.[8] Dedicated GPS devices show where someone has traveled and store the addresses of personal associates or favorite destinations.[9] This Court recently acknowledged "an individual's privacy interests in comprehensive accounts of her movements, in her location, and in the location of her personal property in private spaces." *Graham*, 2015 WL 4637931, *8. While people cannot physically "lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read," they now can do so digitally. *Riley*, 134 S. Ct. at 2489; s*ee also Cotterman*, 709 F.3d at 965 ("digital devices allow us to carry the very papers we once stored at home").

Many digital devices—such as Mr. Saboonchi's smartphones—can permit access to even more personal information stored in the "cloud"—that is, not on the devices themselves, but on servers accessible via the Internet.[10] Border agents could get a comprehensive look at a traveler's financial life with smartphone or tablet "apps" that link to bank, credit card, and retirement accounts, as well as

---

health information includes the user's GPS location and call and text notifications, https://www.fitbit.com/surge.

[8] *See*, *e.g.*, Amazon's Kindle, which "holds thousands of books" as well as personal documents, http://www.amazon.com/dp/B00I15SB16/ref=nav_shopall_k_ki#kindle-compare.

[9] *See*, *e.g.*, Garmin, https://buy.garmin.com/en-US/US/cOnTheRoad-cAutomotive-p1.html.

[10] *See* National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*, Special Publication 800-145 (Sept. 2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

monthly bills.[11] Or they could see inside a traveler's home via live video feeds provided by home security "apps."[12] Some digital devices already store virtually all data in the cloud[13] and one can imagine a time when this will be ubiquitous.[14] Because cloud data can "appear as a seamless part of the digital device when presented at the border," *Cotterman*, 709 F.3d at 965, border agents "would not typically know whether the information they are viewing was stored locally … or has been pulled from the cloud," *Riley*, 134 S. Ct. at 2491. Yet the district court largely dismissed the implications of cloud computing. *Saboonchi I*, 990 F. Supp. 2d at 563-64.

Digital devices differ wildly from luggage and other physical items a person brings on an international trip and has when returning to the United States. Now is the time to acknowledge the full force of the privacy implications of border searches of digital devices because "the rule we adopt must take account of more

---

[11] *See*, *e.g.*, Mint, https://www.mint.com/how-mint-works.
[12] *See*, *e.g.*, NestCam, https://nest.com/camera/meet-nest-cam/.
[13] *See*, *e.g.*, Google's Chromebook ("Gmail, Maps, Docs and pics safely stored in the cloud, so a laptop spill really is just a laptop spill."), https://www.google.com/chromebook/about/.
[14] *See*, *e.g.*, Stephen Lawson, "Future of Mobile Phones Is in the Cloud, Ex-Nokia CTO Says," *InfoWorld* (April 16, 2009), http://www.infoworld.com/article/2631862/mobile-apps/future-of-mobile-phones-is-in-the-cloud--ex-nokia-cto-says.html ("The standard architecture that will realize the promise of mobile phones won't be hardware or software but a cloud-based platform…").

sophisticated systems that are already in use or in development." *Kyllo v. United States*, 533 U.S. 27, 36 (2001).

## II. The Border Search Exception Is Narrow.

"[T]he ultimate touchstone of the Fourth Amendment is reasonableness." *Riley*, 134 S. Ct. at 2482 (citing *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)). When the "primary purpose" of a search is "to detect evidence of ordinary criminal wrongdoing," reasonableness requires a warrant based on probable cause. *City of Indianapolis v. Edmond*, 531 U.S. 32, 38 (2000); *see also Riley*, 134 S. Ct. at 2482 (citing *Vernonia School District 47J v. Acton*, 515 U.S. 646, 653 (1995)). However, the Supreme Court has held that, *in limited circumstances*, neither a warrant nor individualized suspicion is required when the primary purpose of a search is "beyond the normal need for law enforcement" or "beyond the general interest in crime control." *Vernonia*, 515 U.S. at 653; *Edmond*, 531 U.S. at 37, 48. Crucially, searches under these limited exceptions are only reasonable if the purpose of the search is "tethered" to the justifications underlying the exception. *Riley*, 134 S. Ct. at 2485 (citing *Arizona v. Gant*, 556 U.S. 332, 343 (2009)); *see also Florida v. Royer*, 460 U.S. 491, 500 (1983) (warrantless searches "must be limited in scope to that which is justified by the particular purposes served by the exception").

The search-incident-to-arrest exception at issue in *Riley* is not justified by the need to gather additional evidence of the alleged crime, but instead the need to

protect officer safety and prevent the destruction of evidence. *Riley*, 134 S. Ct. at 2483 (citing *Chimel v. California*, 395 U.S. 752 (1969)). The warrantless and suspicionless drug tests at issue in *Vernonia* were upheld as reasonable to protect the health and safety of minor student athletes. 515 U.S. at 665. By contrast, the warrantless and suspicionless vehicle checkpoint in *Edmond* to uncover illegal narcotics was unconstitutional because its primary purpose was to "uncover evidence of ordinary criminal wrongdoing." 531 U.S. at 42.

The border search exception permits warrantless and suspicionless searches of individuals and items in their possession when crossing into the United States. *Id.* at 38-42. *Edmond* clarified that although some warrant exceptions—like border searches—might involve law enforcement activities because they can result in "arrests and criminal prosecutions," that does not mean that the exceptions were "designed primarily to serve the general interest in crime control." *Id.* at 42. Rather, the border search exception is intended to serve the narrow purposes of enforcing the immigration and customs laws. *See Cotterman*, 709 F.3d at 956 (noting "narrow" scope of border search exception).

In 1925, the Supreme Court articulated these two limited justifications for warrantless and suspicionless searches at the border: "Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as *entitled* to

come in, and his belongings as effects which may be *lawfully* brought in." *Carroll v. United States*, 267 U.S. 132, 154 (1925) (emphasis added). *Carroll* cited *Boyd*, which drew a clear distinction between searches and seizures consistent with the purposes of the border search exception—in particular, enforcing customs laws—and those to obtain evidence for a criminal case:

> The search for and seizure of … goods liable to duties and concealed to avoid the payment thereof, are totally different things from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him.

116 U.S. at 623. Outside of the border context and beyond these narrow justifications, *Carroll* rejected the "inconvenience and indignity" of a warrantless and suspicionless search that amounts to a fishing expedition. 267 U.S. at 154.

Accordingly, under the immigration and customs rationales, the border search doctrine may be invoked to prevent undocumented immigrants from entering the United States, *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973), and to enforce the laws regulating the importation of goods into the U.S. and ensuring duties are paid on those goods. *See Boyd*, 116 U.S. at 617. Warrantless and suspicionless border searches are also permitted to prevent the importation of contraband such as drugs, weapons, agricultural products and other physical items that could harm individuals and industries if brought into the country. *See United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971)

(discussing inspecting luggage to "exclude[e] illegal articles from the country."); *United States v. 12 200-Foot Reels of Super 8mm Film*, 413 U.S. 123, 125 (1973) (discussing the need "to prevent smuggling and to prevent prohibited articles from entry"); *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985) (discussing "the collection of duties and prevent the introduction of contraband into this country").[15]

In *United States v. Ramsey*, the Supreme Court made clear that the Constitution places significant restrictions on the border search exception: "The border-search exception is grounded in the recognized right of the sovereign to control, *subject to substantive limitations imposed by the Constitution*, who and what may enter the country." 431 U.S. 606, 620 (1977) (emphasis added). Thus a border search can be "'unreasonable' because of the particularly offensive manner in which it is carried out." *Id.* at 618 n. 13. In *Montoya de Hernandez*, the Supreme Court held that reasonable suspicion is required to detain a traveler until she has defecated to see if she is smuggling drugs in her alimentary canal. 473 U.S. at 541. The Court later noted that *Montoya de Hernandez* generally extends to "highly

[15] *See also* Chad Haddal, *Border Security: Key Agencies and Their Missions*, Congressional Research Service, 2 (January 26, 2010), https://www.fas.org/sgp/crs/homesec/RS21899.pdf ("CRS Report") ("CBP's mission is to prevent terrorists and terrorist weapons from entering the country, provide security at U.S. borders and ports of entry, apprehend illegal immigrants, stem the flow of illegal drugs, and protect American agricultural and economic interests from harmful pests and diseases.").

intrusive searches" that implicate the "dignity and privacy interests of the person being searched." *Flores-Montano*, 541 U.S. at 152.

While *Ramsey* stated that "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border," 431 U.S. at 616, the Court's reliance on *Boyd* and *Carroll* suggests that the Court understood that right to remain tethered to the specific purposes of enforcing the immigration and customs laws. *Id.* at 617-19. This parallels both *Chimel* and *Riley*, which narrowed the search-incident-to-arrest exception by holding that searches of a home and cell phone data were outside the scope of the narrow purposes of the exception. *See Riley*, 134 S. Ct. at 2483 (citing *Chimel*, 395 U.S. at 753-54, 762-63).

Therefore, it is not "anything goes" at the border. *United States v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008) (en banc). Rather, the Fourth Amendment only permits border searches tied to the enforcement of immigration and customs laws.

## III. The Distinction Between "Conventional"/"Routine" and "Forensic" Searches Is Factually Meaningless and Constitutionally Unworkable.

Following the Ninth Circuit in *Cotterman*, the district court held that "forensic" searches of digital devices at the border have significant privacy implications and thus require reasonable suspicion, while "conventional" or "routine" searches fit within the border search exception. *Saboonchi I*, 990 F. Supp.

2d at 547-49; *Saboonchi II*, 48 F. Supp. 3d at 819; *see also Cotterman*, 709 F.3d at 966 (distinguishing "cursory" searches from "exhaustive forensic searches" of digital devices). The district court defined "conventional" or "routine" searches of digital devices as *manual* searches "limited by the amount of time one Customs officer has to devote to reviewing the contents of digital evidence at the border while its owner awaits the outcome of the search." *Saboonchi I*, 990 F. Supp. 2d at 547, 563-64. In the district court's view, the "finite amount of time" for a manual search is an "inherent limitation." *Id.* at 564. "Forensic" searches, by contrast, require the use of sophisticated *software* "over an extended period of time" and usually occur "away from the border." *Id.*

The district court refused to require a warrant based on probable cause for all searches of data on digital devices at the border. Instead, the district court only focused on the privacy implications of "forensic" searches: "Facile analogies of forensic examination of a computer or smartphone to the search of a briefcase, suitcase, or trunk are no more helpful than analogizing a glass of water to an Olympic swimming pool because both involve water located in a physical container." *Saboonchi I*, 990 F. Supp. 2d at 561.

Yet *Riley* did not distinguish between how digital devices are searched or the devices themselves (*i.e.*, Mr. Riley's smartphone and Mr. Wurie's flip phone). The Court required a probable cause warrant for *all searches* of cell phones seized

during an arrest, even though the searches in that case were manual searches—*less* intrusive in the district court's view than the "forensic" searches of Mr. Saboonchi's devices. *Riley*, 134 S. Ct. at 2480-81.

While the district court sought to accommodate the significant privacy interests in digital devices, the dichotomy between "conventional"/"routine" and "forensic" searches is factually meaningless and constitutionally unworkable because any search of a digital device implicates the "dignity and privacy interests of the person being searched." *Flores-Montano*, 541 U.S. at 152; *see also Kim*, 2015 WL 2148070, *19 (stating whether the border search of the defendant's laptop was reasonable does not "turn on the application of an undefined term like 'forensic'").

This Court recently rejected a technological distinction as constitutionally unworkable because the government's conduct had the same Fourth Amendment implications. In *Graham*, this Court found the distinction between real-time tracking using a GPS device and historical cell site location information to be "constitutionally insignificant because the Fourth Amendment is concerned with "the government's investigative conduct, *i.e.*, its decision to seek and inspect [location] records without a warrant." *Graham*, 2015 WL 4637931, *12. Likewise, this Court should reject the district court's conclusion in this case that "forensic" searches of digital devices at the border have different constitutional implications

than "conventional" or "routine" searches. Ultimately, the government's conduct is the same: accessing a tremendous amount of highly personal information without a warrant.

Given the vast amount of highly personal information digital devices contain, including their ability to connect to sensitive data in the cloud, "conventional" or "routine" searches of digital devices at the border implicate privacy interests in ways that manual searches of luggage do not. Even the district court acknowledged that "a conventional computer search can be deeply probing." *Saboonchi I*, 990 F. Supp. 2d at 547. As the cost of storage drops and technology advances, digital devices will hold ever greater amounts of personal information and feature increasingly powerful search capabilities. Manual searches thus will reveal ever more personal information, making the distinction between "conventional"/"routine" and "forensic" searches even more meaningless.[16]

Additionally, technology exists today that enables highly invasive "forensic" searches to be conducted in a more "routine" way—in a relatively brief amount of time and at the border itself—belying not only the district court's focus on time, but also this Court's conclusion in *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005), that "Customs agents have neither the time nor the resources to search the

[16] Apple's iPhone currently has a search function for the entire phone, which pulls up emails, text messages, contacts, notes, calendar events, and reminders based on keywords. Apple, *Search with Spotlight*, https://support.apple.com/en-us/HT201285.

contents of every computer." *Id.* at 507. A company called Cellebrite manufactures several Universal Forensic Extraction Devices or "UFEDs" that plug into cell phones, laptops, tablets and other mobile devices and enable the quick and easy extraction of detailed digital data.[17] UFEDs also enable access to social media accounts and other cloud content, which the company describes as "a virtual goldmine of potential evidence for forensic investigators."[18] UFEDs are small and portable, enabling "simple, real-time extractions onsite."[19] A UFED can extract eight gigabytes of data from an Apple iPhone in a "mere 20 minutes," while its search functions cut the search time "from days to minutes."[20]

---

[17] *See* Cellebrite, *Mobile Forensics Products*, http://www.cellebrite.com/Mobile-Forensics/Products; *UFED Physical Analyzer*, http://www.cellebrite.com/Mobile-Forensics/Applications/ufed-physical-analyzer; *iOS Forensics: Physical Extraction, Decoding and Analysis From iOS Devices*, http://www.cellebrite.com/Pages/ios-forensics-physical-extraction-decoding-and-analysis-from-ios-devices.

[18] Cellebrite, *UFED Cloud Analyzer*, http://www.cellebrite.com/Mobile-Forensics/Applications/ufed-cloud-analyzer.

[19] Cellebrite, *Unlock Digital Intelligence* (2015), http://www.cellebrite.com/Media/Default/Files/Forensics/Solution-Briefs/Mobile-Forensics-Solution-Brief.pdf.

[20] Cellebrite, *Case Study: Cellebrite Certification Training Helps NY Agency Maximize UFED Usage*, http://www.cellebrite.com/Media/Default/Files/Forensics/Case-Studies/Cellebrite-Certification-Training-Helps-NY-Agency-Maximize-UFED-Usage_Case%20Study.pdf.

Customs and Border Protection is already using UFEDs.[21] In training materials, the agency has lauded the devices' portability and ease of use in the field, stressing that no computer is needed to extract data like call logs, videos, pictures and text messages.[22] The FBI also uses UFEDs and prefers this technology due to its "extraction speed and intuitive user interface."[23] Thus, the district court's conclusion that "forensic" searches can never become "conventional" or "routine" because they are more time-consuming and difficult is factually incorrect today. Given the rapid rate of technological change, the district court's conclusion will only become less correct as devices like UFEDs evolve and are able to extract and analyze data even faster.

## IV. A Warrant Based on Probable Cause Should Be Required to Search Data on Digital Devices at the Border.

The Supreme Court in *Riley* declared its preference for "clear guidance" and "categorical rules." 134 S. Ct. at 2491. Given that *Ramsey* noted the similarity

---

[21] Customs and Border Protection, *UFED Kits, Software Updates*, Federal Business Opportunities (Sept. 4, 2013), https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=44c0118f0eea7370c6eb1d5a8bf711d7; Letter from Shari Suzuki, Customs and Border Protection, to Mark Rumold, Electronic Frontier Foundation (May 14, 2012), https://www.eff.org/files/filenode/foia__20120808155244.pdf,

[22] Electronic Frontier Foundation, *CBP Data Extraction Release*, PDF at 31, 33, https://www.eff.org/document/cbp-data-extraction-release.

[23] Federal Bureau of Investigation, *Notice of Intent to Sole Source*, Federal Business Opportunities (Aug. 28, 2013), https://www.fbo.gov/index?s=opportunity&mode=form&id=e3742ca87da9650f719e902f86ad36b6&tab=core&_cview=0.

between the border search exception and the search-incident-to-arrest exception to the warrant requirement, 431 U.S. at 621, this Court should adopt the clear rule that searches of data on digital devices at the border—regardless of how the devices are searched—require a probable cause warrant because of the uniquely personal nature of digital devices and the narrow purposes of the border search exception. Any concerns that a warrant will be difficult to obtain at the border should be allayed given that "[r]ecent technological advances … have … made the process of obtaining a warrant itself more efficient." *Riley*, 134 S. Ct. at 2493.

### A. A Warrant Is Required Given the Highly Personal Information Stored and Accessible on Digital Devices.

The district court declared that digital devices at the border deserve "the highest level of Fourth Amendment protection available." *Saboonchi II*, 48 F. Supp. 3d at 819-20. That level of protection should be a warrant based on probable cause. This categorical rule is appropriate irrespective of how government agents conduct the search.

The district court's rule requiring reasonable suspicion for "forensic" searches of digital devices insufficiently protects Fourth Amendment rights: it exposes digital devices to *warrantless and suspicionless* "conventional" or "routine" searches—conducted manually, in a brief amount of time, and at the border itself while the traveler is waiting—and it exposes those same digital devices to *warrantless* "forensic" searches. Yet manual searches of digital devices are highly

invasive given all the personal data digital devices contain, and CBP is already using sophisticated "forensic" software that can be routinely deployed.

The fact that luggage might contain physical items with sensitive information does not negate the uniquely personal nature of digital devices. The district court stated that "conventional"/"routine" searches of digital devices do not require a warrant or any level of suspicion because "the privacy concerns raised by such a search [do not] differ from where a traveler brings a suitcase full of personal items, files, or a diary." *Saboonchi I*, 990 F. Supp. 2d at 563. However, a few letters in a suitcase do not compare to the detailed record of correspondence over months or years that a digital device may contain and a manual search would reveal, while paper diaries do not have a keyword search function and people do not carry all the diaries they have ever owned when they travel. Moreover, *Riley* rejected that same argument:

> [T]he fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years. And to make matters worse, such an analogue test would allow law enforcement to search a range of items contained on a phone, even though people would be unlikely to carry such a variety of information in physical form.

134 S. Ct. at 2493.

Thus, given that digital devices contain vast amounts of highly personal information, any search is highly invasive and "bears little resemblance" to

searches of travelers' luggage. *Id.* at 2485. Even the Department of Homeland Security acknowledges that "a search of [a] laptop increases the possibility of privacy risks due to the vast amount of information potentially available on electronic devices."[24]

### B. Searching Data on Digital Devices Is Not Tethered to the Narrow Justifications for the Border Search Exception.

An exception to the warrant requirement only applies in a particular situation when doing so would not "untether the rule from the justifications underlying the … exception." *Riley*, 134 S. Ct. at 2485. A rule permitting warrantless and suspicionless searches of data on digital devices at the border would do just that. Given that the primary purpose of searching data on digital devices at the border is almost always ordinary criminal law enforcement, not immigration or customs, government agents must obtain a warrant based on probable cause. Just as with the search-incident-to-arrest exception at issue in *Riley*, the border search exception might "strike[] the appropriate balance in the context of physical objects," but its rationales do not have "much force with respect to digital content on cell phones" or other digital devices. *Id.* at 2484 (citing *United States v. Robinson*, 414 U.S. 218 (1973)).

[24] Department of Homeland Security, *Privacy Impact Assessment for the Border Searches of Electronic Devices*, 2 (Aug. 25, 2009), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf.

*Riley* held that the search-incident-to-arrest exception does not extend to digital devices like cell phones seized pursuant to an arrest. *Id.* at 2485. The Court found that the primary purpose of warrantless and suspicionless searches of data on digital devices seized during an arrest is largely beyond the narrow purposes of the search-incident-to-arrest exception: to protect officers from an arrestee who might grab a weapon, and to prevent him from destroying evidence. *Id.* at 2483, 2485-86. The Court stated that "data on the phone can endanger no one," and the broader possibility that associates of the arrestee will remotely delete digital data does not justify such a significant privacy invasion *in every arrest*. *Id.* at 2485-87.

Likewise, the primary purpose of warrantless and suspicionless searches of digital devices at the border is beyond the narrow purposes of enforcing the immigration and customs laws. A traveler's immigration status is not determined by the personal data on his digital device. Rather, border agents determine a traveler's authority to enter the United States by inspecting physical documents such as a passport and by consulting government databases that contain additional information such as terrorist designations and outstanding arrest warrants.[25]

[25] *See* CRS Report at 2 ("CBP inspectors enforce immigration law by examining and verifying the travel documents of incoming international travelers to ensure they have a legal right to enter the country."); Department of Homeland Security, *Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing* (Dec. 22, 2010), http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf.

Border agents enforce customs laws by interviewing travelers, examining their luggage or vehicles, and if necessary, examining their persons. The traditional purpose of the customs rationale of the border search exception is to prevent *physical items* from entering the country *at the moment* the traveler crosses the border, either because the items were not properly declared for duties or are contraband that could harm individuals or industries if brought into the country, even if an attendant criminal prosecution is authorized by statute. *See Boyd*, 116 U.S. at 617; *12 200-Foot Reels of Super 8mm Film*, 413 U.S. at 124; *Edmond*, 531 U.S. at 42. Physical contraband can never be hidden in digital data—but searching digital data can uncover evidence of ordinary criminal wrongdoing, which requires a probable cause warrant. *Edmond*, 531 U.S. at 38.

Even if some digital content, such as child pornography, is "contraband" that should not enter the country consistent with the customs rationale of the border search exception, this does "not justify dispensing with the warrant requirement across the board." *Riley*, 134 S. Ct. at 2486. In *Riley*, the Court was not persuaded that the search-incident-to-arrest exception should be applied to cell phones because the government had not shown that the problem of losing digital evidence during an arrest is "prevalent." *Id.* Similarly, the border search exception should not be applied to digital devices just because they might contain some digital "contraband." In addition to the significant privacy interests implicated by any

search of a digital device, the government has not demonstrated that digital "contraband"—unlike illegal drugs, for example—is a significant problem *at the border*.[26] Additionally, just as the police can mitigate the risk of losing digital evidence during an arrest by means other than a warrantless search, *Riley*, 134 S. Ct. at 2487 (discussing disconnecting a phone from the network, removing the battery, or placing it in a Faraday bag), the government has more targeted and effective means of combatting the scourge that is child pornography.[27] As the Ninth Circuit said, "legitimate concerns about child pornography do not justify unfettered crime-fighting searches or an unregulated assault on citizens' private information." *Cotterman*, 709 F.3d at 966.

---

[26] Of the 56,218 criminal cases filed in federal court in the 2014 fiscal year, only 102 or .2 percent involved customs violations. *See* United States Department of Justice, *United States Attorney's Annual Statistical Report Fiscal Year 2014*, 11-12, http://www.justice.gov/sites/default/files/usao/pages/attachments/2015/03/23/14statrpt.pdf. In the 2014 fiscal year, child pornography made up only 2.5 percent of all federal "offenders" prosecuted and sentenced in federal court. *See* United States Sentencing Commission, *Overview of Federal Criminal Cases Fiscal Year 2014*, 2, http://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2015/FY14_Overview_Federal_Criminal_Cases.pdf. This represents *all* child pornography offenders, not just those apprehended at the border.

[27] The FBI conducts aggressive undercover online investigations that have resulted in thousands of convictions. Federal Bureau of Investigation, *Overview and History of the Violent Crimes Against Children Program*, https://www.fbi.gov/about-us/investigate/vc_majorthefts/cac/overview-and-history. The FBI and other agencies including Immigration and Customs Enforcement also work closely with NCMEC, which receives tips about child pornography, including from electronic service providers who are legally required to report child pornography to NCMEC. *See* 18 U.S.C. § 2258A; National Center for Missing & Exploited Children, *CyberTipline*, http://www.missingkids.com/CyberTipline.

Indeed, this case vividly demonstrates the dangers of permitting a broad application of the border search exception: the border becomes a predictable place where criminal investigators can obtain troves of evidence without involving the court. Mr. Saboonchi's digital devices were clearly searched for the purpose of ordinary criminal law enforcement. When Mr. Saboonchi was at the Rainbow Bridge border crossing, border agents did not suspect him of having an invalid passport, not declaring goods subject to import duties, or attempting to bring in contraband—physical or digital. The only reason he was sent to secondary screening was because his name came up in the TECS database because he had been under investigation for nearly two years. *Saboonchi I*, 990 F. Supp. 2d at 539, 541. Agent Baird testified that she typically searches digital devices seized at the border for "any evidence of criminality."[28] She confirmed that she wanted to search Mr. Saboonchi's media "to see if there was evidence of export violations" to further an "investigation begun prior to when this stop took place."[29]

The Supreme Court's border search cases were never intended to create a loophole for the government to search for evidence of any criminal activity whenever someone appears at the border. If Agent Baird had wanted to search Mr. Saboonchi's digital devices inside the United States, she would have needed a probable cause warrant. Instead, she sought, as the district court concluded, "to

[28] J.A. 226, line 4.
[29] J.A. 225, lines 24–25; J.A. 220, lines 14–15.

take advantage of the Government's border search authority," *Saboonchi I*, 990 F. Supp. 2d at 543, even though the searches of Mr. Saboonchi's digital devices had nothing to do with the narrow purposes of the border search exception. *See Kim*, 2015 WL 2148070, *22 (holding that a search of Kim's laptop using forensic software was unreasonable given that it was "for the purpose of gathering evidence in a pre-existing [export violation] investigation, was supported by so little suspicion of ongoing or imminent criminal activity, and was so invasive of Kim's privacy and so disconnected from … the considerations underlying the breadth of the government's authority to search at the border").

## V. A Warrant Requirement Does Not Limit the Applicability of Existing Exceptions.

"[T]he warrant requirement is an important working part of our machinery of government, not merely an inconvenience to be somehow weighed against the claims of police efficiency." *Riley*, 134 S. Ct. at 2493 (quotations omitted). Complying with this important constitutional protection will not threaten the government's ability to recover digital data.

Border agents would also still benefit from the border search exception: as in *Riley*, they would not be prohibited from searching without a warrant or individualized suspicion the "physical aspects" of a digital device to ensure that it does not contain contraband such as drugs or explosives. *Riley*, 134 S. Ct. at 2485.

Border agents would also not be prohibited from invoking a separate exception to the warrant requirement, such as exigent circumstances. If an agent has probable cause to believe that a digital device contains criminal evidence and has reasonable suspicion that the traveler will destroy that evidence while maintaining possession of the device, the agent may *seize* the device without a warrant for a reasonable amount of time in order to secure the search warrant and execute the search. *Riley*, 134 S. Ct. at 2488 (discussing "reasonable steps to secure a scene to preserve evidence") (citing *Illinois v. McArthur*, 531 U.S. 326 (2001)). Or, if an agent has probable cause to believe that a digital device contains evidence of criminal activity, and is faced with a "now or never" situation where he has reasonable suspicion that a traveler's cell phone "will be the target of an imminent remote-wipe attempt," the agent may search the device without a warrant. *Id.* at 2487, 2494 (citing *Missouri v. McNeely*, 133 S. Ct. 1552, 1561-62 (2013)).

## CONCLUSION

This Court should adopt the categorical rule that a warrant based on probable cause is required to search the data on digital devices seized at the international border, irrespective of how the government conducts a search. Not only does this provide a clear, workable rule for law enforcement and courts alike, most critically, it protects the "dignity and privacy interests" of travelers entering

the United States. *Flores-Montano*, 541 U.S. at 152. The district court's opinion should be reversed.

Dated: September 10, 2015

*/s/ Sophia Cope*
Sophia Cope
Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Email: sophia@eff.org

*Counsel for Amicus Curiae*
ELECTRONIC FRONTIER FOUNDATION

**CERTIFICATE OF COMPLIANCE**
**WITH TYPE-VOLUME LIMITATION,**
**TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS**
**PURSUANT TO FED. R. APP. P. 32(a)(7)(C)**

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amicus Curiae in Support of Appellant complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,832 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: September 10, 2015

*/s/ Sophia Cope*
Sophia Cope

*Counsel for Amicus Curiae*
ELECTRONIC FRONTIER FOUNDATION

## CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system on September 10, 2015.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: September 10, 2015

*/s/ Sophia Cope*
Sophia Cope

*Counsel for Amicus Curiae*
*Electronic Frontier Foundation*