Case No. 16-4687

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

HAMZA KOLSUZ,

Defendant-Appellant.

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, ASIAN AMERICANS ADVANCING JUSTICE-ASIAN LAW CAUCUS, BRENNAN CENTER FOR JUSTICE, COUNCIL ON AMERICAN-ISLAMIC RELATIONS (CAIR), CAIR CALIFORNIA, CAIR FLORIDA, CAIR MISSOURI, CAIR NEW YORK, CAIR OHIO, CAIR DALLAS/FORT WORTH, AND THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF DEFENDANT-APPELLANT

On Appeal from the U.S. District Court for the Eastern District of Virginia
The Honorable T.S. Ellis, III, Senior U.S. District Court Judge
Case No. 1:16-cr-00053-TSE

Sophia Cope
Counsel of Record
Adam Schwartz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
sophia@eff.org

Counsel for Amici Curiae EFF, AAAJ-ALC, CAIR, and five CAIR Chapters

Michael Price
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
120 Broadway, Suite 1750
New York, New York 10271
(646) 292-8335

Counsel for Amicus Curiae Brennan Center for Justice

Thania Diaz Clevenger
COUNCIL ON AMERICAN-ISLAMIC RELATIONS FLORIDA
8076 N. 56th Street
Tampa, Florida 33617
(813) 514-1414

Counsel for Amicus Curiae CAIR Florida, Inc.

Elizabeth A. Franklin-Best
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
Blume Franklin-Best & Young, LLC
900 Elmwood Avenue, Suite 200
Columbia, South Carolina 29201
(646) 292-8335

Counsel for Amicus Curiae NACDL

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, *amici curiae* Electronic Frontier Foundation, Asian Americans Advancing Justice-Asian Law Caucus, Brennan Center for Justice at NYU School of Law, Council on American-Islamic Relations, Council on American-Islamic Relations California, CAIR Florida, Inc., Council on American-Islamic Relations Missouri, Council on American-Islamic Relations New York, Inc., Council on American-Islamic Relations Ohio, Council on American-Islamic Relations Dallas/Fort Worth, and The National Association of Criminal Defense Lawyers state that they do not have parent corporations, and that no publicly held corporation owns 10% or more of the stock of *amici*.

Dated: March 20, 2017

Respectfully submitted,

/s/ Sophia Cope
Sophia Cope
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Counsel of Record for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

STATEMENT OF INTEREST[1]

Amici Electronic Frontier Foundation,[2] Asian Americans Advancing Justice-Asian Law Caucus,[3] Brennan Center for Justice at NYU School of Law,[4] Council on American-Islamic Relations,[5] Council on American-Islamic Relations California,[6] CAIR Florida, Inc.,[7] Council on American-Islamic Relations Missouri,[8] Council on American-Islamic Relations New York, Inc.,[9] Council on American-Islamic Relations Ohio,[10] Council on American-Islamic Relations Dallas/Fort Worth,[11] and The National Association of Criminal Defense Lawyers[12] are nonprofit public interest organizations that work to protect civil liberties. *Amici* advocate for the constitutional right to privacy, including at the U.S. border.

---

[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 *amici*, 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] eff.org.
[3] advancingjustice-alc.org.
[4] brennancenter.org. This brief does not purport to represent the position of NYU School of Law.
[5] cair.com.
[6] ca.cair.com.
[7] cairflorida.org.
[8] cair-mo.org.
[9] cair-ny.org.
[10] cairohio.com.
[11] cair-dfw.org.
[12] nacdl.org.

INTRODUCTION

The Fourth Amendment's border search exception, permitting warrantless and suspicionless "routine" searches of belongings and persons at the U.S. border, should not apply to digital devices like Mr. Kolsuz's iPhone. All border searches of the data stored or accessible on digital devices—whether "manual" or "forensic"—are "non-routine" and thus fall outside the border search exception. This is because *any search* of digital data is a "highly intrusive" search that implicates the "dignity and privacy interests" of the traveler. *U.S. v. Flores-Montano*, 541 U.S. 149, 152 (2004). Under the Supreme Court's ruling in *Riley v. California,* 134 S. Ct. 2473 (2014), border agents should be required to obtain a probable cause warrant to search the data stored or accessible on a digital device.

The *Riley* Court presented an analytical framework that complements the border search doctrine's traditional consideration of whether a search is "routine" or "non-routine." *See U.S. v. Kolsuz*, 185 F. Supp. 3d 843, 855–56 (E.D. Va. 2016). The Court explained that, in determining whether to apply an existing exception to the warrant and probable cause requirements to a "particular category of effects" such as cell phones, individual privacy interests must be balanced against legitimate governmental interests. *Riley*, 134 S. Ct. at 2484. The government's interests are analyzed by considering whether a search conducted without a warrant and probable cause is sufficiently "tethered" to the purposes

underlying the exception. *Id.* at 2485. In the case of digital data at the border, not only are individual privacy interests at their highest in devices such as cell phones and laptops, searches of digital devices without a warrant and probable cause are not sufficiently "tethered" to the narrow purposes justifying the border search exception: immigration and customs enforcement.

However, even if such "tethering" may be considered sufficient—meaning that there is a clear nexus between enforcing the immigration and customs laws, and conducting searches of digital devices at the border without a warrant and probable cause—the extraordinary privacy interests that travelers have in their cell phones and laptops outweigh any legitimate governmental interests. Prior to the rise of mobile computing, the "amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile." *U.S. v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (en banc). Today, however, the "sum of an individual's private life" sits in the pocket or purse of any traveler carrying a cell phone, laptop or other digital device. *Riley*, 134 S. Ct. at 2489.

The district court below correctly stated that "*Riley* appears to indicate that cell phones deserve the highest level of Fourth Amendment protection available." *Kolsuz*, 185 F. Supp. 3d at 859. However, given that *Riley* did not explicitly involve the border context, the district court erroneously concluded that "the

highest protection available for a border search is reasonable suspicion." *Id.* Thus, the district court adopted the Ninth Circuit's dichotomy in *Cotterman* and held that the "manual" search of Mr. Kolsuz's iPhone was a "routine" border search that fell within the border search exception, while the later "forensic" search of his iPhone with a Cellebrite device was a "non-routine" search that required reasonable suspicion. *Id.* at 858. *See also Cotterman*, 709 F.3d at 968.[13]

Unfortunately, the *Kolsuz* court did not go far enough. A "person's digital life ought not to be hijacked simply by crossing a border." *Cotterman*, 709 F.3d at 965. *Amici* urges this Court to hold that all border searches of the data stored or accessible on digital devices are "non-routine," and thus, consistent with *Riley*, a probable cause warrant is required.

ARGUMENT

I. Digital Devices Contain and Access 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 a cell phone should fall within the

[13] In a border search case that was before this Court prior to being mooted, the district court felt similarly bound by *Riley*'s lack of explicit applicability to the border, and so also adopted the *Cotterman* rule. *U.S. v. Saboonchi* (*Saboonchi II*), 48 F. Supp. 3d 815, 819 (D. Md. 2014) (stating that "a modern cell phone deserves the highest level of Fourth Amendment protection available").

search-incident-to-arrest exception, which permits the warrantless and suspicionless search of an arrestee's cell phone, because the search of cell phone data was supposedly 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. See also U.S. v. Kim*, 103 F. Supp. 3d 32, 55 (D.D.C. 2015) (in a border search case, 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"). The Court examined the nature of cell phones themselves—rather than how the devices are searched—and concluded they 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 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

Most people carry portable digital devices. 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." *Riley*, 134 S. Ct. at 2484. Globally, there are 7.1 billion cell phone subscriptions, including 2.6 billion for a smartphone.[14] Ninety-five percent of American adults

[14] Ericsson, *Ericsson Mobility Report* 2 (June 2015), http://www.ericsson.com/res/docs/2015/ericsson-mobility-report-june-2015.pdf.

own a cell phone, with 77 percent owning a smartphone.[15] Additionally, 22 percent of American adults own an e-reader and 51 percent own a tablet computer.[16] 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.

Digital devices are both quantitatively and qualitatively different from physical containers. *Id.* at 2489. 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. *See also Saboonchi II*, 48 F.Supp.3d at 819 (stating "the sheer quantity of information available on a cell phone makes it unlike other objects to be searched"). 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.").

---

[15] Pew Research Center, *Mobile Technology Fact Sheet* (Jan. 12, 2017), http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.
[16] *Id.*

Qualitatively, digital devices "collect[] in one place many distinct types of information … that reveal much more in combination than any isolated record." *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 phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on." *Riley*, 134 S. Ct. at 2489. Also, "[h]istoric location information is a standard feature on many smartphones 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 *U.S. v. Jones*, 565 U.S. 400, 415 (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.")).

Even digital devices with more limited features and storage capacity than cell phones and laptop computers contain a wide variety of highly personal information. Wearable fitness devices track a variety of data related to an individual's health.[17] E-readers can reveal every book a person has read.[18]

[17] For example, FitBit's Surge records steps, distance, floors climbed, calories burned, active minutes, workouts, sports played, sleep, and heart rate. It also

Dedicated GPS devices, including car navigation systems, show where someone has traveled and store the addresses of personal associates or favorite destinations.[19]

Importantly, many digital devices, such as Mr. Kolsuz's iPhone, permit access to personal information stored in the "cloud"—that is, not on the devices themselves, but on servers accessible via the Internet.[20] Thus, 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 monthly bills.[21] Or they could see inside a traveler's home via live video feeds provided by

---

records non-health information including the user's GPS location, and call and text notifications. *See* Fitbit, *Surge specs*, *https*://www.fitbit.com/surge.

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

[19] *See*, *e.g.*, Garmin, *Drive Product Line*, http://www8.garmin.com/automotive/pdfs/drive.pdf; Nissan, *NissanConnect Navigation System Features*, https://www.nissanusa.com/connect/features-app/navigation-system. Additionally, the next generation of "connected cars"—with Internet access, and a variety of sensors and features—promise to be a treasure trove of data on drivers and their passengers. *See, e.g.,* PwC Strategy&, *Connected Car Report 2016: Opportunities, Risk, and Turmoil on the Road to Autonomous Vehicles* (Sept. 28, 2016), http://www.strategyand.pwc.com/reports/connected-car-2016-study.

[20] *See* National Institute of Standards and Technology, Special Pub. 800-145, *The NIST Definition of Cloud Computing* (Sept. 2011), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[21] *See*, *e.g.*, Mint, *All in One*, https://www.mint.com/how-mint-works.

home security apps.[22] Some digital devices already store virtually all data in the cloud,[23] and some analysts predict this will become ubiquitous.[24] 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. In this case, it is immaterial that Mr. Kolsuz's iPhone was set to airplane mode, "meaning it could not access a cellular network or the Internet," or that the Cellebrite device did not access cloud content. *Kolsuz*, 185 F. Supp. 3d at 849. One toggle by a border agent would have granted access to any cloud content accessible via the iPhone.

Therefore, 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." *Riley*, 134 S. Ct. at 2489. 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

---

[22] *See*, *e.g.*, Nest, *Meet the Nest Cam Indoor Security Camera*, https://nest.com/camera/meet-nest-cam/.

[23] *See*, *e.g.*, Google, *About Chromebook* ("Gmail, Maps, Docs and pics [are] safely stored in the cloud, so a laptop spill really is just a laptop spill"), https://www.google.com/chromebook/about/.

[24] *See*, *e.g.*, Stephen Lawson, *Future of Mobile Phones Is in the Cloud, Ex-Nokia CTO Says*, *InfoWorld* (April 16, 2009) ("The standard architecture that will realize the promise of mobile phones won't be hardware or software but a cloud-based platform…."), http://www.infoworld.com/article/2631862/mobile-apps/future-of-mobile-phones-is-in-the-cloud--ex-nokia-cto-says.html

read," they now do so digitally. *Id.* at 2489. *See also Cotterman*, 709 F.3d at 965 (stating "digital devices allow us to carry the very papers we once stored at home"). The district court correctly stated that "a cell phone cannot fairly be compared to an ordinary container that might be searched at the border because as the Supreme Court in *Riley* made clear, '[a] phone not only contains in digital form many sensitive records previously found in the home,' but also 'a broad array of private information never found in a home in any form….'" *Kolsuz*, 185 F.Supp.3d at 856 (quoting *Riley*, 134 S. Ct. at 2491).

In sum, portable digital devices differ wildly from luggage and other physical items a person possesses when entering or leaving the country. 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 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. Normally, reasonableness requires a warrant based on probable cause. *Id.* (citing *Vernonia School District 47J v. Acton*, 515 U.S. 646, 653 (1995)). However, *in limited circumstances*, neither a warrant nor probable cause 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; *City of Indianapolis v. Edmond*, 531 U.S. 32, 37, 48 (2000). Crucially, searches without a warrant and probable cause (including *suspicionless* searches) under these limited exceptions must be "tethered" to the purposes justifying 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. Warrantless and suspicionless sobriety checkpoints are reasonable because they advance the non-criminal purpose of roadway safety. *Michigan Dept. of State Police v. Sitz,* 496 U.S. 444 (1990). 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." *Edmond*, 531 U.S. at 42.

The border search exception permits warrantless and suspicionless "routine" searches of individuals and items in their possession when crossing the U.S. border. *U.S. v. Montoya de Hernandez*, 473 U.S. 531 (1985). *Edmond* clarified that although some 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." 531 U.S. 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 (emphasizing the "narrow" scope of the 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 [i] himself as *entitled* to come in, and [ii] his belongings as effects which may be *lawfully* brought in." *Carroll v. U.S.*, 267 U.S. 132, 154 (1925) (emphasis added). *Carroll* relied on *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.

Accordingly, under the immigration and customs rationales, the border search exception permits warrantless and suspicionless "routine" searches in order to prevent undocumented immigrants from entering the United States, *Almeida-Sanchez v. U.S.*, 413 U.S. 266, 272 (1973), and to enforce the laws regulating the importation or exportation of goods, including ensuring that duties are paid on those goods, *Boyd*, 116 U.S. at 624. The border search exception may also be invoked to prevent the importation of contraband such as drugs, weapons, agricultural products, and other items that could harm individuals and industries if brought into the country. *See Montoya de Hernandez*, 473 U.S. at 537 (discussing "the collection of duties and … prevent[ing] the introduction of contraband into this country").[25]

While the Supreme Court in *U.S. v. Ramsey* stated that "searches made at the

[25] *See also* Chad Haddal, Cong. Research Serv., 7-5700, *Border Security: Key Agencies and Their Missions* 2 (Jan. 26, 2010) ("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."), https://www.fas.org/sgp/crs/homesec/RS21899.pdf.

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. 606, 616 (1977), the Court's reliance in *Ramsey* on *Boyd* and *Carroll* shows that the Court understood that this government power must remain tethered to the specific purposes of enforcing the immigration and customs laws. *Id.* at 617-19. This parallels both *Chimel* and *Riley*, which held that searches of a home and cell phone data, respectively, were outside the scope of the narrow purposes of the search-incident-to-arrest 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. *U.S. v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008) (en banc). Rather, the Fourth Amendment requires that border searches without a warrant and probable cause must be "tethered" to enforcing the immigration and customs laws.

III. All Border Searches of Digital Devices, Whether "Manual" or "Forensic," are Highly Invasive of Personal Privacy and Are Thus "Non-Routine"

In *Ramsey*, the Supreme Court made clear that the Constitution restricts 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. at

620 (emphasis added). Thus, not all border searches are "routine." The Court has defined "non-routine" border searches as "highly intrusive" or those that impact the "dignity and privacy interests" of travelers, *Flores-Montano*, 541 U.S. at 152, or are carried out in a "particularly offensive manner," *Ramsey*, 431 U.S. at 618 n.13. Thus, in *Montoya de Hernandez*, the Supreme Court held that detaining a traveler until she defecated to see if she was smuggling drugs in her digestive tract was a "non-routine" seizure and search that required reasonable suspicion. 473 U.S. at 541.

In this case, the district court adopted the Ninth Circuit's dichotomy in *Cotterman* and held that the "manual" search of Mr. Kolsuz's iPhone was a "routine" border search, while the later "forensic" search of his iPhone with a Cellebrite device, four miles from the Dulles airport and one month after the phone was seized, was a "non-routine" search that required reasonable suspicion. *Kolsuz*, 185 F. Supp. 3d at 858. While the district court acknowledged that "an individual's privacy interest in the information contained on his cell phone is much greater than an individual's privacy interest in the contents of his luggage or other personal effects," the district court only focused on the privacy implications of the "forensic" search of Mr. Kolsuz's iPhone, calling it "essentially a body cavity search of the cell phone." *Id.* at 856 (citing *U.S. v. Saboonchi* (*Saboonchi I*), 990 F. Supp. 2d 536, 569 (D. Md. 2014)). *See also Cotterman*, 709 F.3d at 966 (referring

to a "forensic" search of a laptop as a "computer strip search").

The district court correctly held that the Cellebrite search of Mr. Kolsuz's iPhone was "non-routine" even though the search did not include creating "a complete bitstream copy" of the phone's hard drive, which would have encompassed unallocated space and thus potentially deleted information, or include accessing cloud content. *Kolsuz*, 185 F. Supp. 3d at 857, 860. It was enough that the Cellebrite search "involved the use of specialized software to copy a large amount of data," resulting in an 896-page report. *Id.* at 857.

However, *any search* of the data on a digital device, whether manually or with specialized "forensic" tools, is a "highly intrusive" search that implicates the "dignity and privacy interests" of the traveler, and thus should be considered "non-routine." *Flores-Montano*, 541 U.S. at 152.

Given the vast amounts of highly personal information digital devices contain, as well as their ability to connect to sensitive data in the cloud, even "manual" searches of digital devices at the border greatly burden privacy interests in ways that searches of luggage do not. *See Saboonchi I*, 990 F.Supp.2d at 547 (acknowledging that "a conventional computer search can be deeply probing"). The Cellebrite search of Mr. Kolsuz's iPhone yielded contact lists, photographs, videos, emails, conversations in messaging apps, calendar entries, web browsing history, call logs, and a history of the iPhone's precise GPS coordinates. *Kolsuz*,

185 F.Supp.3d at 849. A border agent could have easily tapped through Mr. Kolsuz's iPhone and accessed this *same detailed personal information* via a "manual" search.[26] Even a history of a traveler's physical location may be uncovered through a "manual" search: for example, on an iPhone, a user may have toggled on the "Frequent Locations" feature.[27] Or, if a traveler uses Google Maps while logged into their Google account, a "manual" search of the app would reveal the traveler's navigation history.[28] 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.[29] Thus, "manual" searches will reveal ever more personal information, making the distinction between them and "forensic" searches even more meaningless.

Additionally, new technology enables border agents to quickly conduct "forensic" searches at the border itself. This empowers the government to invade the digital privacy of ever growing numbers of travelers. For example, Cellebrite manufactures several Universal Forensic Extraction Devices ("UFEDs") that plug

---

[26] Although he could have accessed more data, the CBP agent decided to only access Mr. Kolsuz's recent text messages and calls during the "manual" search of the iPhone. *Kolsuz*, 185 F.Supp.3d at 848.

[27] To change iOS 10 settings go to Settings>Privacy>Location Services>System Services>Frequent Locations.

[28] *See* Google, *Maps*, https://www.google.com/maps/.

[29] Apple's iPhone currently has a search function for the entire phone that pulls content based on keywords. Apple, *Use Search on Your iPhone, iPad, or iPod Touch*, https://support.apple.com/en-us/HT201285.

into cell phones, laptops, tablets and other mobile devices and enable the quick and easy extraction of detailed digital data.[30] 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."[31] UFEDs are small and portable, enabling "simple, real-time extractions onsite."[32] 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."[33] As this case reveals, CBP is already using UFEDs.[34] In training materials, the agency lauds the devices' portability and ease of use in the field, stressing that no computer is needed to

---

[30] *See* Cellebrite, *Mobile Forensics Products*, http://www.cellebrite.com/Mobile-Forensics/Products; Cellebrite, *UFED Physical Analyzer*, http://www.cellebrite.com/Mobile-Forensics/Applications/ufed-physical-analyzer; Cellebrite, *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.

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

[32] Cellebrite, *Unlock Digital Intelligence* 3 (2015), http://www.cellebrite.com/Media/Default/Files/Forensics/Solution-Briefs/Mobile-Forensics-Solution-Brief.pdf.

[33] Cellebrite, *Case Study: Cellebrite Certification Training Helps NY Agency Maximize UFED Usage* 1, http://www.cellebrite.com/Media/Default/Files/Forensics/Case-Studies/Cellebrite-Certification-Training-Helps-NY-Agency-Maximize-UFED-Usage_Case%20Study.pdf.

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

extract data like call logs, videos, pictures, and text messages.[35] The FBI also uses UFEDs and prefers this technology due to its "extraction speed and intuitive user interface."[36]

Thus, the rapid rate of technological change belies this Court's suggestion more than a decade ago, based on much more primitive technology, that "[c]ustoms agents have neither the time nor the resources to search the contents of every computer." *U.S. v. Ickes*, 393 F.3d 501, 507 (4th Cir. 2005). As the Ninth Circuit noted, "It is the *potential* unfettered dragnet effect that is troublesome." *Cotterman*, 709 F.3d at 966 (emphasis added).

Therefore, the dichotomy between "manual" and "forensic" searches is factually meaningless and constitutionally unworkable. Constitutional rights should not turn on such a flimsy distinction. *See Kim*, 103 F. Supp. 3d at 55 (stating that whether the border search of the defendant's laptop was reasonable does not "turn on the application of an undefined term like 'forensic'"). Importantly, *Riley* did not distinguish between how digital devices are searched. Even though the searches in *Riley* were *manual* searches, the Court required a probable cause warrant for *all searches* of a cell phone seized incident to an arrest.

---

[35] EFF, *CBP Data Extraction Release*, 31, 33, https://www.eff.org/document/cbp-data-extraction-release.

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

Riley, 134 S. Ct. at 2480-81, 2493.

In sum, this Court should reject the district court's conclusion that "manual" searches of digital devices at the border have fewer constitutional implications than "forensic" searches. All searches of digital devices at the border are "non-routine" and thus fall outside the border search exception because the government's conduct is the same: accessing to an unprecedented degree tremendous amounts of highly personal information.

IV. A Probable Cause Warrant Should Be Required for Border Searches of Data Stored or Accessible on Digital Devices

The Supreme Court prefers "clear guidance" and "categorical rules." *Riley*, 134 S. Ct. at 2491. The *Riley* Court's analytical framework complements the border search doctrine's traditional consideration of whether a search is "routine" or "non-routine." *See Kolsuz*, 185 F. Supp. 3d at 855–56. In determining whether to apply an existing exception to the warrant and probable cause requirements to a "particular category of effects," individual privacy interests must be balanced against legitimate governmental interests. *Riley*, 134 S. Ct. at 2484. In the case of border searches of digital devices, this balancing clearly tips in favor of the traveler. Given that *Ramsey* noted the similarity between the border search exception and the search-incident-to-arrest exception, 431 U.S. at 621, this Court should adopt the clear rule that *all* border searches of data stored or accessible on

digital devices are "non-routine" searches that require a probable cause warrant.[37]

Border agents would still benefit from the border search exception: for example, they could search 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. *See Riley*, 134 S. Ct. at 2485. Moreover, 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.[38]

A. A Probable Cause Warrant Should Be Required Given the Highly Personal Information Stored and Accessible on Digital Devices

Modern digital devices like cell phones and laptops reveal the "sum of an individual's private life," *Riley*, 134 S. Ct. at 2489, making any search by the government an unprecedented intrusion into individual privacy. As the district court recognized, "even at the border, an individual has a significant privacy

---

[37] While the Supreme Court's border search cases have not required more than reasonable suspicion for "non-routine" searches, the Court has never said that reasonable suspicion is the absolute upper limit. *See, e.g.*, *Montoya de Hernandez* 473 U.S. at 541 n.4 ("[W]e suggest no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches."). Additionally, while a California district court concluded that it was bound by the Ninth Circuit's ruling in *Cotterman* in a case about a "manual" border search of a cell phone, the court stated, "If it could, this Court would apply *Riley*." *U.S. v. Caballero*, 178 F. Supp. 3d 1008, 1017 (S.D. Cal. 2016).

[38] Border agents clearly have the ability to seek and obtain judicial authorization for non-routine searches and seizures. *See, e.g., Montoya de Hernandez*, 473 U.S. at 535 ("[C]ustoms officials sought a court order authorizing a pregnancy test, an x ray, and a rectal examination.").

interest in the digital contents of his phone." *Kolsuz*, 185 F.Supp.3d at 856.

Nevertheless, the district court only required reasonable suspicion for "forensic" border searches of digital devices. *Id.* at 859. The district court's rule insufficiently protects Fourth Amendment rights: it exposes digital devices to *warrantless* "forensic" searches subject to a lower standard of suspicion, and it exposes those same digital devices, with the same personal information, to *warrantless and suspicionless* "manual" searches. Yet "manual" searches of digital devices are highly intrusive given all the personal information that border agents may access, and CBP is already using sophisticated "forensic" tools that can be rapidly deployed at the border.

Additionally, the fact that luggage may contain physical items with personal information does not negate the unique privacy interests in digital devices. 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 even a "manual" search would reveal. Also, paper diaries do not have a keyword search function and people do not carry all the diaries they have ever owned when they travel. The *Riley* Court rejected this 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, any border search of a digital device is highly intrusive and "bears little resemblance" to searches of travelers' luggage. *Id.* at 2485. Even DHS 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."[39]

Citing *Riley*, the district court declared that digital devices at the border "deserve the highest level of Fourth Amendment protection available." *Kolsuz*, 185 F. Supp. 3d at 859. That level of protection is a probable cause warrant. This categorical rule is necessary irrespective of how border agents conduct a digital device search.

B. A Probable Cause Warrant Should Be Required Because Searching Digital Data Is Not Tethered to the Narrow Purposes of the Border Search Exception

Under the *Riley* balancing test, the government's interests are analyzed by considering whether a search conducted without a warrant or probable cause is "tethered" to the purposes underlying the exception. 134 S. Ct. at 2485. In the case

[39] DHS, *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.

of digital data at the border, searches of digital devices without a warrant and probable cause are not sufficiently "tethered" to the narrow purposes justifying the border search exception: immigration and customs enforcement. As with the search-incident-to-arrest exception, the border search exception might "strike[] the appropriate balance in the context of physical objects," but its underlying rationales do not have "much force with respect to digital content on cell phones" or other digital devices. *Id.* at 2484 (citing *U.S. v. Robinson*, 414 U.S. 218 (1973)).

In creating the categorical rule that the search-incident-to-arrest exception does not extend to digital devices like cell phones, the *Riley* Court found that searches without a warrant and probable cause of data on digital devices seized following an arrest are not sufficiently "tethered" to the narrow purposes of the search-incident-to-arrest exception: to protect officers from an arrestee who might grab a weapon, and to prevent the arrestee from destroying evidence. *Id.* at 2483, 2485-86. The Court stated that "data on the phone can endanger no one," and the probabilities are small that associates of the arrestee will remotely delete digital data or that an officer will discover an unlocked phone in time to thwart a password lock or encryption. *Id.* at 2485-88. The Court concluded that neither "problem is prevalent," and therefore their possibilities do not justify such a significant privacy invasion—that is, a warrantless search of a cell phone—*for every arrest*. *Id.*

Likewise, searches of digital devices at the border without a warrant and probable cause are not sufficiently "tethered" to the narrow purposes of enforcing the immigration and customs laws.

Border agents determine a traveler's immigration status and authority to enter the United States, not by inspecting the personal data on a digital device, but rather by inspecting physical documents such as a passport or visa, and by consulting government databases that contain additional information such as terrorist designations and outstanding arrest warrants.[40]

Border agents enforce customs laws by interviewing travelers, examining their luggage or vehicles, and if necessary, their persons. The traditional purpose of the customs rationale of the border search exception is to prevent physical items from entering (or leaving) the country at the moment the traveler crosses the border, typically because the items were not properly declared for duties, or are contraband that could harm individuals or industries if brought into the country. Physical items cannot be hidden in digital data.

In this case, Mr. Kolsuz is being prosecuted for attempting to export firearms parts to Turkey without a license. *Kolsuz*, 185 F. Supp. 3d at 845. While

[40] *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."); DHS, *Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing* 8–9 (Dec. 22, 2010), http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf.

firearms parts are physical items that were, in fact, found in Mr. Kolsuz's luggage, warrantless searches of Mr. Kolsuz's iPhone are not sufficiently "tethered" to enforcing laws against unlicensed exports. As the district court stated, the government's interest in enforcing export control laws "is not directly implicated" in this case because "the digital contents of a cell phone are not banned by export control regulations." *Id.* at 858. The government argued that "a cell phone may contain digital receipts of weapons parts purchases [or] images of weapons parts." *Id.* The district court countered by stating that "this information is merely indirect evidence of the things an individual seeks to export illegally—not the things themselves—and therefore the government's interest in obtaining this information is less significant than the government's interest in directly discovering the items to be exported illegally." *Id.* The district court concluded "that any digital information contained on a cell phone that is relevant to exporting goods illegally can be easily obtained once a border agent establishes some level of individualized suspicion." *Id.*

Some digital content, such as child pornography, may be considered "digital contraband" that may be interdicted at the U.S. border. *Cf. U.S. v. Thirty-Seven (37) Photographs*, 402 U.S. 363, 376–77 (1971) ("Congress may declare [obscenity] contraband and prohibit its importation."). However, the government has not demonstrated that "digital contraband"—unlike illegal drugs, for

example—is a significant or "prevalent" problem *at the border* that justifies a categorical rule permitting searches of digital devices absent a warrant and probable cause.[41] 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.

Ultimately, even if "tethering" may be considered sufficient—meaning that there is a clear nexus between enforcing the immigration and customs laws, and conducting searches of digital devices at the border without a warrant and probable cause—the extraordinary privacy interests that travelers have in their cell phones and laptops (as discussed above) still outweigh any legitimate governmental interests. Governmental interests do "not justify dispensing with the warrant requirement across the board." *Riley*, 134 S. Ct. at 2486. "The Supreme Court has never endorsed the proposition that the goal of deterring illegal contraband at the border suffices to justify any manner of intrusive search." *Cotterman*, 709 F.3d at

[41] Of the 56,218 criminal cases filed in federal court in the 2014 fiscal year, only 102 or 0.2 percent involved customs violations. *See* DOJ, *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* U.S. Sentencing Commission, *Overview of Federal Criminal Cases Fiscal Year 2014* 2 (Aug. 2015), 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.

967.

CONCLUSION

This Court should adopt the categorical rule that all border searches of data stored or accessible on digital devices are "non-routine," and thus, consistent with *Riley v. California*, a probable cause warrant is required.

Dated: March 20, 2017

Respectfully submitted,

/s/ Sophia Cope
Sophia Cope
Counsel of Record
Adam Schwartz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
sophia@eff.org

Counsel for Amici Curiae EFF, AAAJ-ALC, CAIR, and five CAIR Chapters

Michael Price
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
120 Broadway, Suite 1750
New York, New York 10271
(646) 292-8335

Counsel for Amicus Curiae Brennan Center for Justice

Thania Diaz Clevenger
COUNCIL ON AMERICAN-ISLAMIC
RELATIONS FLORIDA
8076 N. 56th Street
Tampa, Florida 33617
(813) 514-1414

Counsel for Amicus Curiae CAIR Florida, Inc.

Elizabeth A. Franklin-Best
NATIONAL ASSOCIATION OF
CRIMINAL DEFENSE LAWYERS
Blume Franklin-Best & Young, LLC
900 Elmwood Avenue, Suite 200
Columbia, South Carolina 29201
(803) 765-1044

Counsel for Amicus Curiae NACDL

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 *Amici Curiae* in Support of Appellant complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,457 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: March 20, 2017

/s/ Sophia Cope
Sophia Cope

Counsel of Record for Amici Curiae

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 March 20, 2017.

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: March 20, 2017

/s/ Sophia Cope
Sophia Cope

Counsel of Record for Amici Curiae