NO. 17-50151

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

V.

MIGUEL ANGEL CANO,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
for Southern California at San Diego
Case No. 16-cr-01770-BTM-1

The Honorable Barry Ted Moskowitz, Chief District Court Judge

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT

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

Counsel for Amicus Curiae

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 its stock.

TABLE OF CONTENTS

CORPORATE DISCLOSURES ii

TABLE OF CONTENTS iii

TABLE OF AUTHORITIES iv

STATEMENT OF INTEREST 1

INTRODUCTION 2

ARGUMENT 4

I. Digital Devices Contain and Access Vast Amounts of Highly Personal Information 4

II. The Border Search Exception Is Narrow 10

III. All Border Searches of Digital Data, Whether "Manual" or "Forensic," are Highly Intrusive of Personal Privacy and Are Thus "Non-Routine" 14

A. The *Cotterman* Dichotomy is Unworkable Because "Manual" Searches Are Highly Intrusive 15

B. This Court Should Hold That the Use of Cellebrite Technology is a "Forensic" Search and Thus Is "Non-Routine" 18

IV. A Probable Cause Warrant Should Be Required for Border Searches of Data Stored or Accessible on Digital Devices 19

A. A Probable Cause Warrant Should Be Required Given the Highly Personal Information Stored and Accessible on Digital Devices 21

B. A Probable Cause Warrant Should Be Required Because Searching Digital Data Is Not Tethered to the Narrow Purposes of the Border Search Exception 23

CONCLUSION 28

CERTIFICATE OF COMPLIANCE 29

CERTIFICATE OF SERVICE 30

TABLE OF AUTHORITIES

Cases

Almeida-Sanchez v. U.S.,
413 U.S. 266 (1973).....13

Arizona v. Gant,
556 U.S. 332 (2009).....11

Boyd v. U.S.,
116 U.S. 616 (1886).....5, 12, 13, 14

Carroll v. U.S.,
267 U.S. 132 (1925).....12, 14

Chimel v. California,
395 U.S. 752 (1969).....11, 14

City of Indianapolis v. Edmond,
531 U.S. 32, 37 (2000).....11, 12

Florida v. Royer,
460 U.S. 491 (1983).....11

Kyllo v. U.S.,
533 U.S. 27 (2001).....10

Michigan Dept. of State Police v. Sitz,
496 U.S. 444 (1990).....11

Riley v. California,
134 S. Ct. 2473 (2014).....*passim*

U.S. v. Caballero,
178 F. Supp. 3d 1008 (S.D. Cal. 2016).....4

U.S. v. Cano,
222 F. Supp. 3d 876 (S.D. Cal. 2016).....*passim*

U.S. v. Cotterman,
709 F.3d 952 (9th Cir. 2013) .....*passim*

U.S. v. Feiten,
2016 WL 894452 (E.D. Mich. 2016) 19

U.S. v. Flores-Montano,
541 U.S. 149 (2004) 2, 15, 16, 20

U.S. v. Griffith,
867 F.3d 1265 (D.C. Cir. 2017) 21

U.S. v. Jones,
565 U.S. 400 (2012) 7

U.S. v. Kim,
103 F. Supp. 3d 32 (D.D.C. 2015) 5, 17

U.S. v. Kolsuz,
185 F.Supp.3d 843 (E.D. Va. 2016) 15, 19, 25, 26

U.S. v. Molina-Isidoro,
2016 WL 8138926 (W.D. Tex. Oct. 7, 2016) 4, 25

U.S. v. Montoya de Hernandez,
473 U.S. 531 (1985) ..... *passim*

U.S. v. Ramsey,
431 U.S. 606 (1977) 13, 14, 15, 20

U.S. v. Robinson,
414 U.S. 218 (1973) 23

U.S. v. Saboonchi,
48 F.Supp.3d 815 (D. Md. 2014) 6

U.S. v. Saboonchi,
990 F.Supp.2d 536 (D. Md. 2014) 15, 16

U.S. v. Seljan,
547 F.3d 993 (9th Cir. 2008) 14, 15

U.S. v. Thirty-Seven Photographs,
402 U.S. 363 (1971) 26

Vernonia School District 47J v. Acton,
515 U.S. 646 (1995) 10, 11

Constitutional Provisions

U.S. Const., amend. IV ..... *passim*

Other Authorities

Amazon, *Kindle* 8

Apple, *Use Search on Your iPhone, iPad, or iPod Touch* 17

Cellebrite, *Solutions & Products* 19

Chad Haddal, *Border Security: Key Agencies and Their Missions* [7-5700],
Congressional Research Service (Jan. 26, 2010) 13, 24

Department of Homeland Security, *Privacy Impact Assessment for the Border Searches of Electronic Devices* (Aug. 25, 2009) 22

Department of Homeland Security, *Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing* (Dec. 22, 2010) 24

E.D. Cauchi, *Border Patrol Says It's Barred From Searching Cloud Data on Phones*, NBC News (July 12, 2017) 8

EFF, *CBP Responds to Sen. Wyden: Border Agents May Not Search Travelers' Cloud Content* (July 17, 2017) 9

Ericsson, *Ericsson Mobility Report* (June 2017) 6

Fitbit, *Charge 2* 8

Garmin, *Garmin Drive Product Line* 8

Google, *Maps* 17

Mint, *How It Works* 9

Nest, *Nest Cam IQ Indoor* 9

Nissan, *Nissan Navigation System* 8

Peter Mell, Timothy Grance, *The NIST Definition of Cloud Computing* [Special Pub. 800-145], National Institute of Standards and Technology (Sept. 2011).....8

Pew Research Center, *Mobile Technology Fact Sheet* (Jan. 12, 2017).....6

PwC Strategy&, *Connected Car Report 2016: Opportunities, Risk, and Turmoil on the Road to Autonomous Vehicles* (Sept. 28, 2016).....8

U.S. Sentencing Commission, *Overview of Federal Criminal Cases Fiscal Year 2016* (May 2017) 27

STATEMENT OF INTEREST[1]

Amicus curiae Electronic Frontier Foundation (EFF) is a non-profit civil liberties organization with more than 44,000 members that works to protect rights in the digital world. Based in San Francisco and founded in 1990, EFF regularly advocates in courts and broader policy debates on behalf of users and creators of technology in support of free expression, privacy, and innovation. As a recognized expert focusing on the intersection of civil liberties and technology, EFF is particularly concerned with protecting the constitutional right to digital privacy—including at the U.S. border—at a time when technological advances have resulted in an increased ability of the government to pry into the private lives of innocent Americans.

[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. The parties consented to the filing of this brief.

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. Cano's cell phone. 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 impacts 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." 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. *Id.* at 2484. The government's interests are analyzed by considering whether a search of a particular category of property, conducted without a warrant and probable cause, would be 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.

In this case, the district court followed *Cotterman*'s dichotomy between "forensic" and "manual" searches, and held that the two warrantless searches of Mr. Cano's cell phone were "reasonable" under the Fourth Amendment. *U.S. v. Cano*, 222 F. Supp. 3d 876, 882 (S.D. Cal. 2016). The district court held that the first search was a "manual" or "cursory" search, and thus did not require any

individualized suspicion. *Id.* at 882. The second search was conducted using Cellebrite technology. *Id.* at 878. The district court declined to determine whether it was a "forensic search," which would have required reasonable suspicion per *Cotterman*, but instead simply held that border agents had probable cause. *Id.* at 878, 882.

However, a "person's digital life ought not to be hijacked simply by crossing a border." *Cotterman*, 709 F.3d at 965. This Court has an opportunity to revisit the issue of what Fourth Amendment standards apply to digital devices at the border. *Amicus* 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.[2]

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

[2] Another district court in this circuit stated, "If it could, this Court would apply *Riley*." *U.S. v. Caballero*, 178 F. Supp. 3d 1008, 1017, 1018 (S.D. Cal. 2016). *Caballero* is currently on appeal to the Ninth Circuit. *See* Appeal No. 17-50199 (9th Cir.). Similarly, a district court in the Fifth Circuit stated, "Were this Court free to decide this matter in the first instance, it might prefer that a warrant be required to search an individual's cell phone at the border." *U.S. v. Molina-Isidoro*, 2016 WL 8138926, *8 (W.D. Tex. Oct. 7, 2016). *Molina-Isidoro* is currently on appeal to the Fifth Circuit. *See* Appeal No. 17-50070 (5th Cir.).

general matter to constitute only a narrow intrusion on privacy." *Riley*, 134 S. Ct. at 2489. In *Riley*, the government argued that a search of cell phone data is the same as a search of physical items, and so a cell phone should fall within the search-incident-to-arrest exception, which would permit the warrantless and suspicionless search of an arrestee's cell phone. *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 *Riley* 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. U.S.*, 116 U.S. 616, 630 (1886)).

Most people carry mobile 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 7.5 billion cell phone subscriptions,

including 3.9 billion for a smartphone.[3] Ninety-five percent of American adults own a cell phone, with 77 percent owning a smartphone.[4] Additionally, 22 percent of American adults own an e-reader and 51 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.

Digital devices are both quantitatively and qualitatively different from physical containers like luggage. *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 U.S. v. Saboonchi*, 48 F.Supp.3d 815, 819 (D. Md. 2014) (*Saboonchi II*) (stating "the sheer quantity of information available on a cell phone makes it unlike other objects to be searched"). With their "immense storage capacity," cell phones, laptops, tablets and other digital devices can contain the equivalent of "millions of pages of text, thousands of pictures, or hundreds of

[3] Ericsson, *Ericsson Mobility Report* (June 2017), https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf.
[4] Pew Research Center, *Mobile Technology Fact Sheet* (Jan. 12, 2017), http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.
[5] *Id.*

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.").

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 laptops contain a wide variety of highly personal information. Wearable fitness devices track an array of data related to an individual's health and

activity.[6] E-readers can reveal every book a person has read.[7] Dedicated GPS devices, including car navigation systems, show where someone has traveled and store the addresses of personal associates and favorite destinations.[8]

Importantly, many digital devices, including smartphones, permit access to personal information stored in the "cloud"—that is, not on the devices themselves, but on servers accessible via the Internet.[9] While CBP announced earlier this year that its agents will not search cloud content,[10] media reports indicate that CBP

---

[6] For example, FitBit's Charge 2 records heart rate, steps, distance, calories burned, active minutes, floors climbed, workouts, hourly activity and stationary time, sleep, and meditation. It also contains non-health information including the user's GPS location, and call, text, and calendar notifications. *See* Fitbit, *Charge 2*, https://www.fitbit.com/shop/charge2?activeFeature=specs.

[7] For example, Amazon's Kindle "holds thousands of books" as well as personal documents. *See* Amazon, *Kindle*, https://www.amazon.com/dp/B00ZV9PXP2/.

[8] *See*, *e.g.*, Garmin, *Garmin Drive Product Line*, https://static.garmincdn.com/emea/com/sites/drive/docs/uk/drive-brochure-2017.pdf; Nissan, *Nissan Navigation System*, 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* 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.

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

[10] E.D. Cauchi, *Border Patrol Says It's Barred From Searching Cloud Data on Phones*, NBC News (July 12, 2017), http://www.nbcnews.com/news/us-news/border-patrol-says-it-s-barred-searching-cloud-data-phones-n782416.

agents have done so,[11] and CBP itself might reverse course. By using devices as portals to cloud content, agents could see inside a traveler's home via live video feeds provided by a home security application ("app").[12] Or officers could get a comprehensive look at a traveler's financial life with an app that links to online bank, credit card, and retirement accounts, as well as monthly bills.[13] Depending on how an app is designed and configured, copies of cloud data may be temporarily stored on a device itself, allowing access even when the device is not connected to the Internet. When a device is connected to the Internet, cloud data can "appear as a seamless part of the digital device when presented at the border," *Cotterman*, 709 F.3d at 965, and thus 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.

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

[11] EFF, *CBP Responds to Sen. Wyden: Border Agents May Not Search Travelers' Cloud Content* (July 17, 2017), https://www.eff.org/deeplinks/2017/07/cbp-responds-sen- wyden-border-agents-may-not-search-travelers-cloud-content.
[12] *See, e.g.*, Nest, *Nest Cam IQ Indoor*, https://nest.com/cameras/nest-cam-iq-indoor/overview/.
[13] *See*, *e.g.*, Mint, *How It Works*, https://www.mint.com/how-mint-works.

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"). But it is not just that a phone "contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Riley*, 134 S. Ct. at 2491.

In sum, digital devices differ wildly from luggage and other physical items a person carries across the border. Now is the time to acknowledge the full force of the privacy implications of border searches of digital devices. As the Supreme Court said, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo v. U.S.*, 533 U.S. 27, 33-34 (2001). Thus, "the rule [a court] adopt[s] must take account of more sophisticated systems that are already in use or in development." *Id.* at 36.

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 under these limited exceptions—without a warrant and probable cause, including *suspicionless* searches—cannot be "untether[ed]" from the purposes justifying the exceptions. *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, not to find evidence to prosecute drug crimes. 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." 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 country, *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, infested agricultural products, and other items that could harm individuals or 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").[14]

While the Supreme Court in *U.S. v. Ramsey* stated that "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by

[14] *See also* Chad Haddal, *Border Security: Key Agencies and Their Missions* [7-5700], Congressional Research Service, 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.

stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border," the *Ramsey* Court's reliance on *Boyd* and *Carroll* shows that the Court understood that this governmental power must remain "tethered" to the specific and narrow purposes of enforcing the immigration and customs laws. 431 U.S. 606, 616-19 (1977). This parallels both *Chimel* and *Riley*, which held that searches of a home and of 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 Data, Whether "Manual" or "Forensic," are Highly Intrusive of Personal Privacy and Are Thus "Non-Routine"

Not all border searches are "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). The Court has defined "non-routine" border searches as those that are "highly intrusive" and 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. *See also Seljan*, 547 F.3d at 1000 ("there might be searches that are so intrusive, destructive, or offensive that they would be deemed unreasonable under the Fourth Amendment"). 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 that she was a drug mule. 473 U.S. at 541.

A. The *Cotterman* Dichotomy is Unworkable Because "Manual" Searches Are Highly Intrusive

This Court concluded in *Cotterman*, 709 F.3d at 967-68, that only "forensic" searches of digital data are "non-routine" (and thus require reasonable suspicion), while "manual" searches of the same data are "routine" and fall within the border search exception (which permits suspicionless searches). *Accord U.S. v. Kolsuz*, 185 F.Supp.3d 843, 858 (E.D. Va. 2016); *U.S. v. Saboonchi*, 990 F.Supp.2d 536, 547-48 (D. Md. 2014) (*Saboonchi I*). In this case, the district court followed *Cotterman* and held that the two warrantless searches of Mr. Cano's cell phone—one "manual" and one conducted using Cellebrite technology—were "reasonable" under the Fourth Amendment. *Cano*, 222 F. Supp. 3d at 882.

However, *any* search of the data stored or accessible on a digital device—whether "manual" or conducted with specialized "forensic" tools—is a "non-

routine" search: it is "highly intrusive" and impacts the "dignity and privacy interests" of the traveler, and is "particularly offensive." *Flores-Montano*, 541 U.S. at 152, 154 n.2. While *amicus* agrees with this Court that "the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy," we do not agree that "forensic" searches "intrude[] upon privacy and dignity interests to a far greater degree than a cursory search," *Cotterman*, 709 F.3d at 966, such that a legal distinction should be made between the two types of searches.

Given the vast amount of highly personal information that digital devices contain, as well as their ability to connect to sensitive data in the cloud, "manual" searches of digital devices at the border greatly burden privacy interests. *See Saboonchi I*, 990 F.Supp.2d at 547 (acknowledging that "a conventional computer search can be deeply probing"). While "manual" searches cannot access deleted files, *see Cotterman* 709 F.3d at 958 n.5, they can access emails, voicemails, text messages, call logs, contact lists, photographs, videos, calendar entries, shopping lists, personal notes, and web browsing history, as well as cloud data via apps. 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.[15] 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.[16]

The rapid rate of technological change will enable "manual" searches to reveal ever more personal information, making the distinction between them and "forensic" searches even more meaningless. As the cost of storage drops and technology advances, travelers' digital devices will hold greater amounts of personal information and feature increasingly powerful search capabilities.[17] This Court should be just as troubled by the "potential unfettered dragnet" of "manual" searches as of "forensic" searches. *See Cotterman*, 709 F.3d at 966.

Therefore, the dichotomy between "manual" and "forensic" searches is factually meaningless and constitutionally unworkable. "Manual" searches can effectively be just as intrusive as "forensic" searches. 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

[15] To change iOS 10 settings go to Settings>Privacy>Location Services>System Services>Frequent Locations.
[16] *See* Google, *Maps*, https://www.google.com/maps/.
[17] Apple's iPhone currently has a search function that pulls content based on keywords. Apple, *Use Search on Your iPhone, iPad, or iPod Touch*, https://support.apple.com/en-us/HT201285.

Riley were "manual" searches (like the first search of Mr. Cano's cell phone), the Court required a probable cause warrant for *all searches* of a cell phone seized incident to an arrest. *Riley*, 134 S. Ct. at 2480-81, 2493.

In sum, *all* searches of digital data at the border are "non-routine" and thus fall outside the border search exception because the government's conduct is the same in both a "manual" and a "forensic" search: accessing to an unprecedented degree tremendous amounts of highly personal information.

B. This Court Should Hold That the Use of Cellebrite Technology is a "Forensic" Search and Thus Is "Non-Routine"

If this Court is persuaded that the government must meet a higher burden only for a "forensic" search, this Court should hold that the use of Cellebrite technology is a "forensic" search.

The second time CBP agents searched Mr. Cano's cell phone, they used Cellebrite technology. *Cano*, 222 F. Supp. 3d at 878. The district court declined to determine whether this second search was "forensic," but instead simply held that the search was justified by probable cause. *Id.* at 878, 882.

A Cellebrite search of a digital device is unequivocally a "forensic" search. This Court in *Cotterman* defined a "forensic" search as one that involves the "application of computer software to analyze a hard drive." 709 F.3d at 967. Cellebrite manufactures several software-based Universal Forensic Extraction Devices ("UFEDs") that plug into cell phones, laptops, tablets, and other mobile

devices, and enable the quick and easy extraction of digital data.[18] The district court in *Kolsuz* concluded that the use of Cellebrite technology, which "involved the use of specialized software to copy a large amount of data," was a "forensic" search and thus "non-routine." 185 F. Supp. 3d at 857, 860.

In *U.S. v. Feiten*, 2016 WL 894452, *6 (E.D. Mich. 2016), the district court erroneously held that the use of OS Triage software was "routine." The court reasoned that this powerful tool supposedly was "*less* invasive of personal privacy" than a "manual" search because it provides "thumbnail preview[s] of pictures and videos on a computer and can identify which of those pictures and videos have file names that match known file names of child pornography." *Id.* (emphasis in original). This reasoning lacks merit, for all the reasons above.

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." 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. Similarly, the district court below stated that

[18] *See* Cellebrite, *Solutions & Products*, https://www.cellebrite.com/en/product/.

border searches must be evaluated by considering the "degree of intrusiveness in light of the sovereign's interest at the border." *Cano*, 222 F. Supp. 3d at 880.

In the case of border searches of digital "effects" such as cell phones and laptops, this balancing clearly tips in favor of the traveler. *Ramsey* recognized the similarity between the border search exception and the search-incident-to-arrest exception, 431 U.S. at 621, and *Flores-Montano* "again [left] open the question 'whether, and under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out,'" 541 U.S. at 154 n.2 (citing *Ramsey*, 431 U.S. at 618 n.13). *See also Cotterman*, 709 F.3d at 963.

Thus, this Court should adopt the clear rule that warrantless and suspicionless border searches of digital devices are unreasonable—specifically, that *all* border searches of data stored or accessible on digital devices are "non-routine" searches that require a probable cause warrant.[19]

Border agents may still benefit from the border search exception: for example, they can search without a warrant or individualized suspicion the "physical aspects" of a digital device, such as the battery compartment, to ensure

[19] 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 for searches conducted at the border. *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.").

that it does not contain contraband such as drugs or explosives. *See Riley*, 134 S. Ct. at 2485. Moreover, any concerns that a warrant is 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.[20]

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 invasion of individual privacy requiring a probable cause warrant. Any border search of a digital device—whether a "manual" search or a "forensic" Cellebrite search, both of which Mr. Cano suffered—is highly intrusive and "bears little resemblance" to searches of travelers' luggage. *Id.* at 2485.[21]

---

[20] 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.").

[21] The district court concluded that the discovery of cocaine in Mr. Cano's spare tire gave border agents probable cause to conduct the second search of his cell phone with Cellebrite technology. *Cano*, 222 F. Supp. 3d at 882. This was not enough: the district court should have required a warrant. The district court also should have required probable cause to believe that there was data *on the digital device* indicating a violation of an immigration or customs law, and not simply probable cause to believe that Mr. Cano violated an immigration or customs law. *Cf. U.S. v. Griffith*, 867 F.3d 1265, 1274 (D.C. Cir. 2017) ("Because a cell phone,

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. As the *Riley* Court explained:

> [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.

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."[22]

---

unlike drugs or other contraband, is not inherently illegal, there must be reason to believe that a phone may contain evidence of the crime.").

[22] 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.

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 category of searches conducted without a warrant and probable cause is "tethered" to the purposes underlying the warrant exception. 134 S. Ct. at 2485. Here, searches of digital devices at the border 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 digital devices seized during an arrest are not sufficiently "tethered" to the narrow purposes of the search-incident-to-arrest exception, namely: 1) to protect officers from an arrestee who might grab a weapon, and 2) to prevent the arrestee from destroying evidence. *Id.* at 2483, 2485-86. In other words, warrantless cell phone searches incident to arrest do not sufficiently advance these goals. The Court stated that 1) "data on the phone can

endanger no one," and 2) the probabilities are low that associates of the arrestee will remotely delete digital data. *Id.* at 2485-88. The Court concluded that neither problem is "prevalent," and that any possibilities do not justify a categorical rule allowing such a significant privacy invasion—that is, permitting a warrantless and suspicionless search of a cell phone *for every arrest*. *Id.*

Likewise here, border searches of digital devices without a warrant and probable cause are not sufficiently "tethered" to the narrow purposes of the border search exception. That is, warrantless border searches of digital devices do not sufficiently advance the goals 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 official documents such as a passport or visa, and by consulting government databases that contain additional information such as outstanding arrest warrants and watchlist designations.[23]

Border agents enforce customs laws by interviewing travelers, examining their luggage or vehicles, and if necessary, their persons. The purpose of the customs rationale of the border search exception is to prevent physical items from

[23] *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,* 8 (Dec. 22, 2010), http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf.

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. Just as the *Riley* Court stated that "data on the phone can endanger no one," 134 S. Ct. at 2485, physical items cannot be hidden in digital data.

Similarly, two district courts recognized the weak "tethering" between warrantless border searches of digital devices and enforcing the immigration and customs laws. In *Molina-Isidoro*, a case involving the attempted smuggling of drugs into the country, the district court stated that a warrantless search of "the contents of a cell phone does not seem to directly contribute to [one] justification for the border search exception—i.e., preventing the entry of unwanted illicit substances into the country." 2016 WL 8138926, *8 n.10. And in *Kolsuz*, a case involving the attempted export without a license of firearms parts, the district court stated that digital data "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." 185 F. Supp. 3d at 858. The *Kolsuz* 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.*

In this case, the warrantless searches of Mr. Cano's cell phone were excessively attenuated from the interdiction of contraband and other customs enforcement.[24] While cocaine was, in fact, found in Mr. Cano's vehicle, the warrantless searches of Mr. Cano's cell phone—like warrantless border searches of digital data generally—were not sufficiently "tethered" to enforcing laws against importing illegal drugs. Mr. Cano rightly argued that the warrantless searches of his cell phone were unreasonable, particularly once the cocaine was found and the phone was seized, as they were "performed [] to gather evidence in an ongoing criminal investigation." *Cano*, 222 F. Supp. 3d at 879. The government admitted that border agents searched Mr. Cano's cell phone to prepare for their interview of him, and to seek possible communications that might lead to hypothetical co-conspirators. *Id.* at 881.

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

[24] Mr. Cano correctly argued that the justifications for the border search exception are "preventing the entry of unwanted persons or contraband." *Cano*, 222 F. Supp. 3d at 879.

demonstrated that "digital contraband"—unlike illegal drugs, for example—is a significant or "prevalent" problem (in the words of the *Riley* Court) *at the border* that justifies a *categorical rule* generally permitting border searches of digital devices absent a warrant and probable cause.[25] This is underscored by the fact that "digital contraband," unlike physical contraband, can be transported across borders via the Internet. As this Court stated, "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 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. As this Court stated, "The Supreme Court has never

[25] In fiscal year 2016, child pornography made up only 2.9 percent of all federal offenders prosecuted and sentenced in federal court. This represents *all* child pornography offenders, not just those apprehended at the border. *See* U.S. Sentencing Commission, *Overview of Federal Criminal Cases Fiscal Year 2016*, 2 (May 2017), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2017/FY16_Overview_Federal_Criminal_Cases.pdf.

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 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*, a probable cause warrant is required.

Dated: January 19, 2018

By: /s/ *Sophia Cope*

Sophia Cope
Adam Schwartz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
sophia@eff.org

Counsel for 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* Electronic Frontier Foundation In Support of Defendant-Appellant complies with the type-volume limitation, because this brief contains 6,585 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: January 19, 2018

By: /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 Ninth Circuit by using the appellate CM/ECF system on January 19, 2018.

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: January 19, 2018

By: /s/ Sophia Cope
Sophia Cope

Counsel for Amicus Curiae
Electronic Frontier Foundation