NO. 18-1299

IN THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

v.

DERRICK LUCIUS WILLIAMS, JR.,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
for the District of Colorado – Denver
No. 16-cr-249-WJM
The Honorable William J. Martinez, United States District Court Judge

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

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

Counsel for Amicus Curiae
Electronic Frontier Foundation

CORPORATE DISCLOSURE STATEMENT

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

TABLE OF AUTHORITIES

Cases

Other Authorities

STATEMENT OF INTEREST[1]

Amicus Curiae Electronic Frontier Foundation is a member-supported, non-profit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 37,000 members. EFF has done extensive work to highlight the unprecedented and significant threats to personal privacy posed by border searches of digital devices, including writing numerous *amicus* briefs, blog posts, and a whitepaper.[2]

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

[2] *See generally* https://www.eff.org/issues/border-searches.

INTRODUCTION

Digital is different. The Fourth Amendment's border search exception, permitting warrantless searches and suspicionless "routine" searches of belongings and persons at the U.S. border, should not apply to digital devices like Mr. Williams' laptop and cell phone.[3] All border searches of the data stored 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). Following the Supreme Court's analysis 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 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 warrant exception to a "particular category of effects" such as cell phones, individual privacy interests must be balanced against legitimate governmental interests. *Id.* at 2484-85. The government's interests are analyzed by considering

[3] Both devices were searched by border agents, but the motion to suppress only relates to the contents found on Mr. Williams' laptop. *U.S. v. Williams*, No. 16-cr-249-WJM, ECF 41 (D. Colo. Sept. 25, 2017) ("*Williams*") at 11.

whether warrantless, suspicionless searches of a particular category of property are 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 zenith in devices such as cell phones and laptops, warrantless, suspicionless searches of digital devices are not sufficiently "tethered" to the narrow purposes justifying the border search exception: immigration and customs enforcement. That is, warrantless, suspicionless searches of digital devices at the border are not necessary to and do not sufficiently advance these goals.

However, even if such "tethering" may be considered sufficient, the unprecedented privacy interests that travelers have in their digital devices 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 erred in denying Williams' motion to suppress the contents found on his laptop. *Williams* at 24. In so doing, the court wrongly assumed that reasonable suspicion is the highest level of privacy protection that digital devices may enjoy at the border, and that no suspicion is ever required for a

"manual" search. *Id.* at 18-19. The district court then found that reasonable suspicion existed, and concluded on this basis that it did not need to decide whether the Fourth Amendment requires reasonable suspicion for a "forensic search," or whether the software-facilitated search of Williams' laptop was a "forensic" search. *Id.* at 9, 18-19.

However, a "person's digital life ought not to be hijacked simply by crossing a border." *Cotterman*, 709 F.3d at 965. *Amicus* urges this Court to hold that all border searches of the data stored on digital devices are "non-routine," and thus, consistent with *Riley*, a probable cause warrant is required.[4]

ARGUMENT

I. Digital Devices Contain Vast Amounts of Highly Personal Information

Before the digital revolution, 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 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

[4] District courts have supported a warrant requirement for border device searches. *See, e.g., U.S. v. Caballero*, 178 F. Supp. 3d 1008, 1017, 1018 (S.D. Cal. 2016) ("If it could, this Court would apply *Riley*."); *U.S. v. Molina-Isidoro*, 267 F. Supp. 3d 900, 909 (W.D. Tex. 2016), *aff'd*, 884 F.3d 287 (5th Cir. 2018) ("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.").

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 digital devices everywhere they go. 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 7.9 billion cell phone subscriptions, including 5 billion for a smartphone.[5] Ninety-five percent of American adults own a cell phone, with 77 percent owning a smartphone.[6]

---

[5] Ericsson, *Ericsson Mobility Report* (Nov. 2018), at 4, 7, https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-november-2018.pdf.

[6] Pew Research Center, *Mobile Fact Sheet* (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/.

Additionally, 73 percent own a laptop or desktop computer.[7] "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 differ fundamentally—in quantitative and qualitative senses—from physical containers like luggage. *Id.* at 2489. *Accord Williams* at 18 n.4.

Quantitatively, "the sheer quantity of information available on a cell phone makes it unlike other objects to be searched." *U.S. v. Saboonchi*, 48 F.Supp.3d 815, 819 (D. Md. 2014) ("*Saboonchi II*"). 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 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."). The district court in this case acknowledged that "digital devices can (and usually do) hold the equivalent of warehouses worth of private information about their owners." *Williams* at 18.

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

[7] *Id*.

Riley, 134 S. Ct. at 2489. This information can include call logs, emails, text messages, voicemails, browsing history, calendar entries, contact lists, shopping lists, notes, photos and videos, and other personal files. *See Riley*, 134 S. Ct. at 2489. This information, in turn, can reveal an individual's political affiliations, religious beliefs and practices, sexual and romantic lives, financial status, health conditions, and family and professional associations. Digital devices "are simultaneously offices and personal diaries" and "contain the most intimate details of our lives." *Cotterman*, 709 F.3d at 964. Additionally, "[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." *Riley*, 134 S. Ct. 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.[8] E-readers can reveal every book a person has read.[9] Dedicated GPS devices, including car navigation systems, show where someone has traveled and store the addresses of personal associates and favorite destinations.[10]

Additionally, 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.[11] CBP announced in 2018 that its agents may not search cloud content.[12] However, depending on how an app or browser is designed and configured, copies of cloud data may be temporarily stored or cached

---

[8] For example, FitBit's Charge 3 records heart rate, calories burned, steps, distance, floors climbed, active minutes, workouts, sleep, and female menstruation and ovulation. It also contains non-health information including the user's GPS location, and call, text, and calendar notifications. *See* Fitbit, *Charge 3*, https://www.fitbit.com/shop/charge3.

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

[10] *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.

[11] *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.

[12] U.S. Customs and Border Protection, *Border Search of Electronic Devices, Directive No. 3340-049A* (Jan. 4, 2018), § 5.1.2, https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.

on the device itself, thereby revealing even more information.[13]

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 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 cell 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, because digital devices differ wildly from luggage and other physical items that travelers carry across the border, border searches of digital devices have extraordinary privacy implications. As the Supreme Court stated, "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).

---

[13] *See* Lee Bell, *What is caching and how does it work?*, Wired UK (May 7, 2017), https://www.wired.co.uk/article/caching-cached-data-explained-delete.

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.* However, warrant exceptions may be justified when legitimate governmental interests outweigh individual privacy interests. *Id.* at 2484. Suspicionless searches, in particular, have been justified where the "primary purpose" of a search is "beyond the normal need for law enforcement" or "beyond the general interest in crime control." *Vernonia School District 47J v. Acton*, 515 U.S. 646, 653 (1995); *City of Indianapolis v. Edmond*, 531 U.S. 32, 37, 48 (2000). Crucially, warrantless and suspicionless searches in a particular context cannot be "untether[ed]" from the purposes justifying the exception at issue. *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, 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, 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, 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 searches 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 two 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 focused border searches to enforce customs laws and unfocused border searches to obtain evidence of crime:

> 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, the border search exception permits warrantless, suspicionless 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]

[14] *See also* Congressional Research Service, *Border Security: Key Agencies and Their Missions* [7-5700] (Jan. 26, 2010) at 2 ("CBP's mission is to prevent

Not to the contrary is *U.S. v. Ramsey*, which stated that "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." 431 U.S. 606, 616 (1977). *Ramsey*'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. *Id.* at 616-18. 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, under the Fourth Amendment, warrantless, suspicionless border searches 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

---

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.

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. 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 smuggler. 473 U.S. at 541. Similarly, the district court below stated that border searches must be evaluated by considering the "degree of intrusiveness." *Williams* at 14 (citing *U.S. v. Uribe-Galindo*, 990 F.2d 522, 525 (10th Cir. 1993)).

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

In 2013 (before *Riley*), the Ninth Circuit in *Cotterman* was the first appellate court to conclude 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). 709 F.3d at 967-68. *Accord U.S. v. Saboonchi*, 990 F.Supp.2d 536, 547-48 (D. Md. 2014) ("*Saboonchi I*"). Similarly, the district court

in this case concluded that the border search doctrine permitted the software-facilitated search of Williams' laptop because, according to the court, the search was supported by reasonable suspicion. *Williams* at 19.

However, *any* search of the data stored on a digital device—whether "manual" or "forensic"—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. It is not true 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. In fact, the district court in this case stated in general that it is "quite natural[] to see searches of personal digital devices as highly intrusive." *Williams* at 18.

Given the vast amounts of highly personal information that digital devices contain, "manual" searches of digital devices at the border greatly burden privacy interests by accessing effectively the same data as "forensic" searches. *See Saboonchi I*, 990 F.Supp.2d at 547 (acknowledging that "a conventional computer search can be deeply probing"). Unlike "manual" searches, "forensic" searches can access deleted files. *See Cotterman* 709 F.3d at 958 n.5; *U.S. v. Kolsuz*, 185 F. Supp. 3d 843, 849 n.8 (E.D. Va. 2016), *aff'd*, 890 F.3d 133 (4th Cir. 2018). However, "manual" searches can access call logs, emails, text messages,

voicemails, browsing history, calendar entries, contact lists, shopping lists, notes, photos and videos, and other personal files that can reveal highly sensitive information about individuals. 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 "Significant 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] Travelers' digital devices increasingly feature expanded hard drive capacities and powerful search capabilities.[17] Thus, 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 immaterial.

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'"). The risk of an "unfettered dragnet," *Cotterman*, 709 F.3d at 966, is just as real for "manual"

[15] For Apple iOS 12: Settings>Privacy>Location Services>System Services>Significant 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.

searches as for "forensic" searches. Importantly, even though the searches in *Riley* were "manual," 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.

In sum, *all* searches of digital data at the border—both "manual" and "forensic"— are "non-routine" and thus fall outside the border search exception.

B. This Court Should Hold That the Use of Software to Copy and Analyze a Device Hard Drive is a "Forensic" Search That Is "Non-Routine"

If this Court is persuaded that the government must meet a higher burden only for a "forensic" search, then this Court should hold that using software to create a "bit-for-bit copy" or image of Mr. Williams' laptop hard drive and then analyzing it with EnCase software—to any degree—was a "forensic" search. *See Williams* at 9, 18-19.

The Ninth Circuit 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. The district court in *Kolsuz* concluded that the "use of specialized software to copy a large amount of data," was a "forensic" and thus "non-routine" border search. 185 F. Supp. 3d at 857, 860.[18] EnCase's manufacturer explains that EnCase

[18] 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

is "digital investigation software" that "helps [government] acquire more evidence than any product on the market" and then analyze that data with "industry-leading processing capabilities."[19]

The district court erred by not expressly holding that the software-facilitated search of Mr. Williams' laptop was a "forensic" search. The court considered that it might be "more like a manual search" because using software to image the hard drive, and thereby bypass the device password, was simply like cutting a luggage lock, and because the government agent used EnCase to search "through active files and directories only." *Williams* at 18. However, after the government breaks a luggage lock, searches the luggage, and then sends the owner on their way, the government no longer has access to the contents of the luggage; but by making a "bit-for-bit" copy of a device hard drive, the government maintains continuing access to its vast quantities of data. The district court seemed to contemplate this fact when it stated that the software-facilitated search of Mr. Williams' laptop could be a "forensic" search because the software helped "recreate the file structure," thereby enabling the government to "search the data at will, including deleted files if desired." *Id.* at 19.

---

names that match known file names of child pornography." *Id.* (emphasis in original).

[19] *See* Guidance Software/OpenText, *EnCase Forensic*, https://www.guidancesoftware.com/encase-forensic.

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

Reasonable suspicion is not the highest standard that may apply to the extraordinarily invasive "non-routine" searches ("manual" and "forensic") of travelers' digital devices. The Supreme Court has never suggested that the reasonable suspicion it required in *Montoya de Hernandez* is a ceiling for every border search, or that property searches can never require heightened protection. Rather, the Court's border search decisions establish reasonable suspicion as the *floor* for highly intrusive searches. *See Montoya de Hernandez,* 473 U.S. at 541 n.4 ("today we 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"); *Flores-Montano*, 541 U.S. at 152; *House v. Napolitano*, 2012 WL 1038816, *7 (D. Mass. 2012) (recognizing the "Supreme Court has not explicitly held that all property searches" at the border never require suspicion).

The *Riley* Court's analytical framework complements the border search doctrine's traditional consideration of whether a search is "routine" or "non-routine."[20] In determining whether to apply an existing warrant exception to a "particular category of effects," individual privacy interests must be balanced against legitimate governmental interests. *Riley*, 134 S. Ct. at 2484-85. In the case

[20] The Supreme Court has recognized the similarity between the border search exception and the search-incident-to-arrest exception. *Ramsey*, 431 U.S. at 621.

of border searches of digital "effects" such as cell phones and laptops, this balancing clearly tips in favor of the traveler.

The Supreme Court prefers "clear guidance" and "categorical rules." *Id.* at 2491. Thus, this Court should adopt the clear rule that *all* border searches of data stored on digital devices are "non-routine" searches that require a probable cause warrant.[21] It is worth noting that *Riley* rejected requiring reasonable suspicion for cell phone searches incident to arrest. *Id.* at 2492.

The Fourth Circuit was the first federal appellate court to hold post-*Riley* that certain border device searches require some level of suspicion about the traveler. In doing so, the court linked the "non-routine" component of the border search doctrine and *Riley*, holding that "under *Riley*, the forensic examination of Kolsuz's phone must be considered a nonroutine border search, requiring some measure of individualized suspicion." *U.S. v. Kolsuz*, 890 F.3d 133, 137 (4th Cir. 2018). The Fourth Circuit declined to hold what the level of suspicion should be;

[21] A warrant should not be difficult to obtain at the border. "Recent technological advances … have … made the process of obtaining a warrant itself more efficient." *Riley*, 134 S. Ct. at 2493. Border agents clearly know how to 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."). In this case, border agents eventually obtained a warrant to conduct a "detailed forensic analysis of the hard drive image." *Williams* at 10-11. Moreover, 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 a laptop battery compartment, to ensure that it does not contain contraband such as drugs or explosives. *See Riley*, 134 S. Ct. at 2485.

though, unlike *Cotterman*, the court left open the possibility of a warrant requirement for both "forensic" and "manual" searches. *Id.* at 137, 141. *See also U.S. v. Molina-Isidoro*, 884 F.3d 287, 292 (5th Cir. 2018) (declining to rule on whether *Riley* requires a warrant for border device searches, but emphasizing that a leading Fourth Amendment legal treatise recognizes that "*Riley* may prompt a reassessment" of the question); *U.S. v. Vergara*, 884 F.3d 1309, 1313 (11th Cir. 2018) (Pryor, J., dissenting) (concluding that "a forensic search of a cell phone at the border requires a warrant supported by probable cause.").

A. A Probable Cause Warrant Should Be Required Given the Highly Personal Information Stored 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 extraordinary invasion of individual privacy requiring a probable cause warrant. Any border search of a digital device—whether a "manual" or "forensic" search—is highly intrusive and "bears little resemblance" to searches of travelers' luggage. *Id.* at 2485. In the context of border device searches, the Fourth Circuit recognized "the Supreme Court's … decision in *Riley* and its emphasis on the significant privacy interests in the digital contents of phones." *Kolsuz*, 890 F.3d at 140.

The fact that luggage may contain physical items with personal information does not negate the unique and significant privacy interests in digital devices. For

example, a letter in a suitcase does not compare to the detailed record of correspondence via email or text message over months or years that a cell phone may contain and even a "manual" search would reveal. Nor does paper correspondence have a keyword search function, and people do not carry all the letters they have ever exchanged when they travel. *See Riley*, 134 S. Ct. at 2493.

The Supreme Court's recent landmark decision in *Carpenter v. U.S.* also informs the border search doctrine. In that case, the Court held that the government must obtain a probable cause warrant for historical cell phone location information maintained by cell phone service providers. 138 S. Ct. 2206, 2221 (2018). The *Carpenter* Court extensively relied on *Riley* in examining the significant privacy interests that individuals have in a record of their physical movements. Of course, historical location information can also be obtained from a border search of a cell phone.

Citing *Riley*, the *Carpenter* Court stated, "When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents." *Carpenter*, 138 S. Ct. at 2222. Similarly, the border search exception should not be extended to digital devices. *See Alasaad v. Nielsen*, 2018 WL 2170323, *20 (D. Mass. 2018) (denying government's motion to dismiss, and relying on *Riley* to hold that "digital searches are different … since they 'implicate privacy concerns far beyond those implicated' in a typical

container search"); *Kim*, 103 F. Supp. 3d at 59 (granting defendant's motion to suppress evidence obtained from a forensic border search of laptop, and relying on *Riley* to hold that laptop search "was so invasive of Kim's privacy"). Even DHS acknowledges that there is a privacy risk in border searches of digital devices "due to the volume of the information that is either stored on, or accessible by, today's electronic devices."[22]

B. A Probable Cause Warrant Should Be Required Because Warrantless, Suspicionless Border Searches of Digital Data Are 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 warrantless, suspicionless searches of a particular category of property are sufficiently "tethered" to the purposes underlying the warrant exception. 134 S. Ct. at 2485. In creating the categorical rule that the search-incident-to-arrest exception does not extend to cell phones, *Riley* found that warrantless, suspicionless searches of cell phones seized during an arrest are not sufficiently "tethered" to the narrow purposes of the search-incident-to-arrest exception: 1) to protect officers from an arrestee who might use a weapon against them, and 2) to prevent the destruction of evidence. *Id.* at 2483, 2485-86. The Court reasoned that 1) "data on the phone can endanger no one," and 2) the

[22] Department of Homeland Security, *Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices, DHS/CBP/PIA-008(a)*, at 2 (Jan. 4, 2018), https://www.dhs.gov/publication/border-searches-electronic-devices.

probability is small that associates of the arrestee will remotely delete digital data. *Id.* at 2485-88. Regarding the latter concern, the Court emphasized that the problem is not "prevalent," and that a possibility does not justify a categorical rule allowing such a significant privacy invasion—that is, permitting a warrantless, suspicionless search of a cell phone *for every arrest*. *Id.*

Likewise, warrantless, suspicionless searches of digital devices at the border are not sufficiently "tethered" to the narrow purposes justifying the border search exception: immigration and customs enforcement. That is, warrantless, suspicionless searches of digital devices at the border are not necessary to and do not sufficiently advance these goals. *See U.S. v. Wurie*, 728 F.3d 1, 13 (1st Cir. 2013), *aff'd*, *Riley*, 134 S. Ct. 2473. 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. *Riley*, 134 S. Ct. at 2484.

Border agents determine a traveler's immigration status and authority to enter the United States by questioning travelers and inspecting official documents such as passports and visas, and border agents enforce customs laws by searching travelers' luggage, vehicles, and, if necessary, their persons. *See*, *e.g.*, *Flores-Montano*, 541 U.S. at 151; *U.S. v. Molina-Gomez*, 781 F.3d 13, 16–17 (1st Cir.

2015). The purpose of the customs rationale of the border search exception, in particular, 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. 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.

Two federal appellate court judges have recognized the weak "tethering" between warrantless, suspicionless 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, Fifth Circuit Judge Gregg Costa in his concurring opinion stated, "Detection of … contraband is the strongest historic rationale for the border search exception." Yet, "[m]ost contraband, the drugs in this case being an example, cannot be stored within the data of a cell phone." He concluded, "this detection-of-contraband justification would not seem to apply to an electronic search of a cellphone or computer." *Molina-Isidoro*, 267 F. Supp. 3d at 295 (Costa, J., concurring). He was also skeptical of a new "evidence-gathering justification" to support warrantless, suspicionless border searches of digital devices. He explained that *Boyd*'s "emphatic distinction between the sovereign's historic interest in

seizing imported contraband and its lesser interest in seizing records revealing unlawful importation has potential ramifications for the application of the border-search authority to electronic data that cannot conceal contraband and that, to a much greater degree than the papers in *Boyd*, contains information that is like an extension of the individual's mind." *Id.* at 297 (internal quotations omitted).

In *Vergara*, Eleventh Circuit Judge Jill Pryor similarly stated, "the rationales underlying the border search exception lose force when applied to forensic cell phone searches… [C]ell phones do not contain the physical contraband that border searches traditionally have prevented from crossing the border." *Vergara*, 884 F.3d at 1317 (Pryor, J., dissenting). Also, similar to Judge Costa, she determined that a new "general law enforcement justification" does not support conducting warrantless, suspicionless cell phone searches at the border. She stated that this justification is "quite far removed from the purpose originally underlying the border search exception: 'protecting the Nation from entrants who may bring anything harmful into this country.'" She concluded, quoting *Riley*, "Excepting forensic cell phone searches from the warrant requirement because those searches may produce evidence helpful in future criminal investigations would thus 'untether the rule from [its] justifications.'" *Id.* at 1317. *See also Kolsuz*, 185 F. Supp. 3d at 858 (digital data "is merely indirect evidence of the things an individual seeks to export illegally—not the things themselves").

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, unlike physical contraband, digital contraband can easily be transported across borders via the Internet. Thus, "it is not clear that the ability to conduct a warrantless search would make much of a difference" in preventing its importation into the country. *Riley*, 134 S. Ct. at 2487. *See also Vergara*, 884 F.3d at 1317 (Pryor, J., dissenting) (stating that "electronic contraband is borderless"). Thus, the government cannot demonstrate that any digital contraband that might be on travelers' devices is a "prevalent" problem (in the words of *Riley*) *at the border* that justifies a *categorical rule* permitting warrantless, suspicionless border searches of all digital devices entering or exiting the country.[23] "[L]egitimate 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 here, the

[23] "The vast majority of child pornography offenders today use the Internet or Internet-related technologies to access and distribute child pornography." *Alasaad*, 2018 WL 2170323, *19, quoting U.S. Sent'g Comm'n, *Federal Child Pornography Offenses* (2012), at 41-42, https://www.ussc.gov/sites/default/files/pdf/news/congressional-testimony-and-reports/sex-offense-topics/201212-federal-child-pornography-offenses/Full_Report_to_Congress.pdf.

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. "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 967.

CONCLUSION

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

Dated: January 3, 2019

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

Counsel for Amicus Curiae Electronic Frontier Foundation

CERTIFICATE OF COMPLIANCE WITH RULE 29(A)(5)

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) because:

[X] this brief contains 6,491 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(f), or

[ ] this brief uses a monospaced typeface and contains [less than 650] lines of text, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(f)

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:

[X] this brief has been prepared in a proportionally spaced typeface using [Microsoft Word 2010] in [14 point Times New Roman font], or

[ ] this brief has been prepared in a monospaced typeface using [name and version of word processing program] with [number of characters per inch and name of type style].

Dated: January 3, 2019

By: */s/ Sophia Cope*
Sophia Cope

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF DIGITAL SUBMISSION

I hereby certify that with respect to the foregoing:

(1) all required privacy redactions have been made per 10th Cir. R. 25.5;

(2) if required to file additional hard copies, that the ECF submission is an exact copy of those documents;

(3) the digital submissions have been scanned for viruses with the most recent version of a commercial virus-scanning program, Avast Mac Security Version 13.11, updated December 19, 2018, and according to the program are free of viruses.

Dated: January 3, 2019

By: */s/ Sophia Cope*
Sophia Cope

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF SERVICE

I hereby certify that on this 3rd day of January, 2019, I electronically filed the foregoing Brief of Amicus Curiae, using the court's CM/ECF system, which will send notification of such filing to the following:

Marissa Rose Miller, marissa.miller@usdoj.gov

Josh Lee, Josh_Lee@fd.org

Dated: January 3, 2019

By: /s/ Sophia Cope

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

Counsel for Amicus Curiae Electronic Frontier Foundation