No. 18-1973

UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

UNITED STATES OF AMERICA

Plaintiff–Appellee,

v.

DONALD WANJIKU

Defendant–Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, ACLU OF ILLINOIS, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT SEEKING REVERSAL

Adam Schwartz
Sophia Cope
Aaron Mackey
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333
Fax: (415) 436-9993
adam@eff.org

Rebecca Glenberg
ROGER BALDWIN FOUNDATION OF ACLU, INC.
180 N. Michigan Ave., Suite 2300
Chicago, IL 60601
Phone: (312) 201-9740
rglenberg@aclu-il.org

Esha Bhandari
Nathan Freed Wessler
Hugh Handeyside
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., Floor 18
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ebhandari@aclu.org

CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 18-1973

Short Caption: United States v. Wanjiku

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief. Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.

[ ] PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P 26.1 by completing item #3):

American Civil Liberties Union ("ACLU")

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Esha Bhandari, Hugh Handeyside, Nathan Freed Wessler, American Civil Liberties Union Foundation

Rebecca Glenberg, Roger Baldwin Foundation of ACLU, Inc.

Sophia Cope, Aaron Mackey, Adam Schwartz, Electronic Frontier Foundation

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

The ACLU, ACLU of Illinois, and the EFF are non-profit entities that do not have parent corporations.

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

No publicly held company owns 10 percent or more of stock in the ACLU, ACLU of Illinois, or EFF.

Attorney's Signature: /s/ Esha Bhandari Date: July 18, 2018

Attorney's Printed Name: Esha Bhandari

Please indicate if you are Counsel of Record for the above listed parties pursuant to Circuit Rule 3(d). Yes X No _____

Address: American Civil Liberties Union
125 Broad Street, 18th Floor, New York, NY 10004

Phone Number: (212) 549-2500 Fax Number: (212) 549-2654

E-Mail Address: ebhandari@aclu.org

CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 18-1973

Short Caption: United States v. Wanjiku

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief. Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.

[ ] PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P 26.1 by completing item #3):

ACLU of Illinois

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Esha Bhandari, Hugh Handeyside, Nathan Freed Wessler, American Civil Liberties Union Foundation

Rebecca Glenberg, Roger Baldwin Foundation of ACLU, Inc.

Sophia Cope, Aaron Mackey, Adam Schwartz, Electronic Frontier Foundation

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

The ACLU, ACLU of Illinois, and the EFF are non-profit entities that do not have parent corporations.

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

No publicly held company owns 10 percent or more of stock in the ACLU, ACLU of Illinois, or EFF.

Attorney's Signature: /s/ Rebecca Glenberg Date: July 18, 2018

Attorney's Printed Name: Rebecca Glenberg

Please indicate if you are Counsel of Record for the above listed parties pursuant to Circuit Rule 3(d). Yes _____ No X

Address: Roger Baldwin Foundation of ACLU, Inc., 180 N. Michigan Ave., Suite 2300, Chicago, IL 60601

Phone Number: (312) 201-9740 Fax Number: (312) 201-9760

E-Mail Address: rglenberg@aclu-il.org

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 18-1973

Short Caption: United States of America v. Donald Wanjiku

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

[ ] **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P 26.1 by completing item #3):

Electronic Frontier Foundation ("EFF")

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Esha Bhandari, Hugh Handeyside, Nathan Freed Wessler, American Civil Liberties Union Foundation

Rebecca Glenberg, Roger Baldwin Foundation of ACLU, Inc.

Sophia Cope, Aaron Mackey, Adam Schwartz, Electronic Frontier Foundation

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

The ACLU, ACLU of Illinois, and EFF are non-profit entities that do not have parent corporations.

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

No publicly held company owns 10 percent or more of stock in the ACLU, ACLU of Illinois, or EFF.

Attorney's Signature: s/ Sophia Cope Date: July 18, 2018

Attorney's Printed Name: Sophia Cope

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** ____ **No** X

Address: Electronic Frontier Foundation
815 Eddy Street, San Francisco, California 94109

Phone Number: (415) 436-9333 Fax Number: (415) 436-9993

E-Mail Address: sophia@eff.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTEREST OF *AMICI CURIAE*[1]

The American Civil Liberties Union ("ACLU") is a nationwide, non-profit, non-partisan organization of nearly 2 million members dedicated to defending the civil liberties and civil rights guaranteed by the Constitution. The ACLU of Illinois is the Illinois state affiliate of the national ACLU. The Electronic Frontier Foundation ("EFF") is a non-profit public interest organization that works to ensure that constitutional rights are protected as technology advances.

The ACLU and EFF have served as *amicus* or counsel in a number of cases involving application of the Fourth Amendment to searches of electronic devices at the border.

[1] Counsel for *amici curiae* certifies that no counsel for a party authored this brief in whole or in part, and no person other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission. The Plaintiff-Appellee and the Defendant-Appellant consent to the filing of this brief.

SUMMARY OF ARGUMENT

This case presents an important question about the extent of Fourth Amendment privacy rights in the digital age. Like Defendant-Appellant Donald Wanjiku, most people carry mobile electronic devices with them when they travel, including when they cross the nation's borders. Those devices contain an incredible volume and variety of intimate information. Yet the government asserts the authority to search such devices without any individualized suspicion, much less a warrant, whenever an individual seeks to enter or exit the country, effectively treating our capacious electronic devices the same as garden-variety physical luggage for Fourth Amendment purposes. As the Supreme Court made clear in *Riley v. California*, 134 S. Ct. 2473 (2014), however, traditional exceptions to the Fourth Amendment's warrant requirement do not automatically apply to searches of cell phones and other electronic devices. Just as warrantless searches of cell phones were not justified by the purposes of the search-incident-to-arrest exception in *Riley*, searches of electronic devices are likewise not justified by the rationales permitting warrantless border searches—namely, immigration and customs enforcement.

The facts of this case demonstrate that warrantless device searches at the border can be used for dragnet investigative purposes and are not properly covered by the border search exception to the warrant requirement because of the immense

privacy interests at stake. As part of a special operation deemed "Operation Culprit," aimed at identifying individuals who had engaged in sex tourism abroad, U.S. Customs and Border Protection ("CBP") officers selected Mr. Wanjiku for secondary inspection and a search of his electronic devices, which included a cell phone, laptop, and external hard drive. App .10. Mr. Wanjiku was initially singled out for a search based on screening criteria that included being a U.S. citizen male, between the ages of 18 and 60, with a prior arrest, who was traveling alone from a country described as being an area of "high sex tourism." *Id*. During the inspection of Mr. Wanjiku's electronic devices, government agents did the following: 1) they "manually 'scroll[ed] through pictures'" on his phone, 2) performed a "forensic 'preview'" of his external hard drive using specialized software that enabled an agent to see a "gallery view" of all the images and videos on the device, 3) searched his cell phone's images and videos using specialized software that can extract data, and 4) searched the images and videos on his laptop using specialized equipment. App. 16–19. These searches were as invasive as the searches for which the Supreme Court required a warrant in *Riley*—and those were manual searches. *See Riley*, 134 S. Ct. at 2480–81 (describing officers viewing photos, videos, and a call log on suspects' phones). Without the protections of a warrant, such conduct is constitutionally impermissible because warrantless searches of electronic devices

infringe too deeply on privacy interests and do not serve the limited purposes of the border search exception to the Fourth Amendment's warrant requirement.

Amici offer this brief to provide greater context about the growing practice of suspicionless and warrantless border searches of electronic devices nationwide. The instant brief provides information about the magnitude of the privacy harm made possible by border agents' easy access to travelers' devices and the implications of the Court's decision in this case for the hundreds of millions of innocent travelers who cross the U.S. border each year—including the many millions who enter and exit the country within this Court's jurisdiction—carrying laptops, smartphones, and other electronic devices that have "immense storage capacity." *Riley*, 134 S. Ct. at 2489.

This Court should hold that searches of electronic devices may not be conducted without a warrant based on probable cause given the significant and unprecedented privacy interests at stake. The information on electronic devices can be deeply sensitive and private, including personal correspondence, notes and journal entries, family photos, medical records, lists of associates and contacts, proprietary business information, attorney-client and other privileged communications, and more. In light of evidence that the number of device searches at the border is increasing, the failure to articulate the appropriate standard may result in a "significant diminution of privacy" for travelers. *Riley*, 134 S. Ct. at

2493. For these reasons, this Court should hold that federal agents violated the Fourth Amendment by searching Mr. Wanjiku's electronic devices without a warrant based on probable cause.

ARGUMENT

I. Border Searches of Electronic Devices Are Increasing Rapidly and Affect Large Numbers of Travelers.

Each year, hundreds of millions of people travel through border crossings, international airports, and other ports of entry into the United States.[2] Of those, tens of thousands of individuals have their electronic devices confiscated, detained, and searched. The Department of Homeland Security has justified its practice of searching electronic devices in part by noting "how infrequent[ly such] searches are conducted,"[3] but border searches of electronic devices have more than tripled in two years. According to data from CBP, the agency conducted 30,200 device searches in fiscal year 2017 as compared to just 8,503 searches in fiscal year 2015.[4]

---

[2] *See* U.S. Customs and Border Protection, *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics* (Jan. 5, 2018) [hereinafter "*CBP FY17 Statistics*"], https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and (more than 397 million international travelers processed in fiscal year 2017).

[3] *See* Mary Ellen Callahan, U.S. Dep't of Homeland Sec., *Privacy Issues in Border Searches of Electronic Devices* 3 (2009), https://www.dhs.gov/sites/default/files/publications/privacy_privacy_issues_border_searches_electronic_devices.pdf.

[4] *See CBP FY17 Statistics*, *supra*; U.S. Customs and Border Protection, *CBP Releases Statistics on Border Device Searches* (Apr. 11, 2017),

The government claims the authority to search international travelers' electronic devices without any particularized or individualized suspicion, let alone a search warrant or probable cause. CBP and U.S. Immigration and Customs Enforcement ("ICE"), which includes Homeland Security Investigations ("HSI"), both have formal policies permitting border officials to search information on electronic devices without a warrant or individualized suspicion—including legal or privileged information, information carried by journalists, medical information, confidential business information, and other sensitive information. *See* U.S. Customs and Border Protection, *Border Search of Electronic Devices*, Directive No. 3340-049A (Jan. 4, 2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf [hereinafter "CBP Policy"]; U.S. Immigration and Customs Enforcement, *Border Searches of Electronic Devices*, Directive No. 7-6.1 § 6.1 (Aug. 18, 2009), http://www.dhs.gov/sites/default/files/publications/7-6.1%20directive.pdf [hereinafter "ICE Policy"].

ICE's policy, issued in 2009, authorizes ICE agents to search electronic devices "with or without individualized suspicion." ICE Policy §§ 6.1, 8.6(1).

---

https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0.

CBP's policy, updated in 2018, never requires a warrant or probable cause for device searches at the border. Rather, for what it deems an "advanced search," in which "external equipment" is connected to the device, it requires either "reasonable suspicion of activity in violation of the laws enforced or administered by CBP" or a "national security concern." CBP Policy § 5.1.4. CBP policy allows any other device search (a "basic" search) "with or without suspicion." *Id*. at § 5.1.3.

The effect of CBP's and ICE's policies is significant, both because of the number of international travelers, and because of the volume and variety of sensitive information contained on or accessible from their electronic devices.

Use of mobile electronic devices is pervasive. Nearly every American adult owns a cell phone of some kind. *See* Pew Research Ctr., *Mobile Fact Sheet* (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/ [hereinafter "Pew Mobile Fact Sheet] (noting 95 percent prevalence). Today, 77 percent of American adults own a smartphone, and rates of smartphone ownership are even higher among younger Americans[5]—who travel internationally at increasingly high rates.[6] People rely on these devices for communication (via text messages, calls, email, and social

[5] Pew Mobile Fact Sheet.

[6] Tanya Mohn, *Travel Boom: Young Tourists Spent $217 Billion Last Year, More Growth Than Any Other Group*, Forbes (Oct. 7, 2013), http://www.forbes.com/sites/tanyamohn/2013/10/07/the-new-young-traveler-boom/.

networking), navigation, entertainment, news, photography, and a multitude of other functions.[7] In addition, more than 10 percent of American adults use a smartphone as their sole means of accessing the Internet at home, meaning that everything they do online—from sending email to searching Google to banking—may be accessible through a single mobile electronic device.[8] Other types of mobile electronic devices also have high rates of use: more than 80 percent of U.S. households have a laptop computer and 54 percent own a tablet.[9]

People consistently carry these devices with them, including when they travel. Mobile devices serve "as digital umbilical cords to what travelers leave behind at home or at work, indispensable travel accessories in their own right, and safety nets to protect against the risks of traveling abroad." *United States v. Saboonchi*, 990 F. Supp. 2d 536, 557–58 (D. Md. 2014).

In light of the ubiquity of electronic devices and the government's claim of sweeping power to search them without suspicion or a warrant at the border, this Court should take the opportunity to clarify the scope of the Fourth Amendment's protections.

---

[7] *See, e.g.*, Aaron Smith, Pew Research Ctr., *U.S. Smartphone Use in 2015, Chapter Three: A "Week in the Life" Analysis of Smartphone Users* (2015), http://www.pewinternet.org/2015/04/01/chapter-three-a-week-in-the-life-analysis-of-smartphone-users/.

[8] Pew Mobile Fact Sheet.

[9] Deloitte, *Digital Democracy Survey* 5 (9th ed. 2015), https://perma.cc/MX5G-2MKG.

II. Warrantless, Suspicionless Searches of Electronic Devices at the Border Violate the Fourth Amendment.

The significant and unprecedented privacy interests that people possess in the contents of their cell phones, laptops, and other electronic devices make warrantless, suspicionless border searches of those devices unconstitutional. As the Supreme Court explained in *Riley*, electronic devices are unlike any other physical containers, given their "immense storage capacity" and the "highly personal" nature of the information they contain. *Riley*, 134 S. Ct. at 2489–90. In *Carpenter v. United States*, the Supreme Court reaffirmed that the rights protected by the Fourth Amendment must not be left to "the mercy of advancing technology," and that the Fourth Amendment protects against "too permeating police surveillance." 138 S. Ct. 2206, 2214 (2018). Accordingly, this Court must reject a "'mechanical interpretation' of the Fourth Amendment" and instead "seek[] to secure 'the privacies of life' against 'arbitrary power.'" *Id*.

Warrantless device searches must receive searching constitutional scrutiny, even when they are undertaken in a context where a traditional exception to the warrant requirement would otherwise apply. *Riley*, 134 S. Ct. at 2484–85. Thus, even at the border, suspicionless and warrantless searches of electronic devices are constitutionally unreasonable. To rule otherwise would give the government unfettered access to an incredible compendium of the most intimate aspects of people's lives simply because they have decided to travel internationally.

A. The Fourth Amendment Requires a Warrant to Search the Contents of an Electronic Device at the Border.

i. The Supreme Court's Analysis in *Riley v. California* Dictates That a Warrant Is Required.

In *Riley v. California*, the Supreme Court made clear that traditional exceptions to the Fourth Amendment's warrant requirement do not automatically extend to searches of digital data. Rather, in determining whether a warrant exception applies, the Constitution requires balancing individual privacy interests against legitimate governmental interests. *Riley*, 134 S. Ct. at 2484–85. *Riley* held that the search-incident-to-arrest exception does not apply to cell phones for two reasons: first, individuals have unique privacy interests in the contents of cell phones; and second, warrantless searches of cell phones are not sufficiently "tethered" to the underlying rationales for the search-incident-to-arrest exception because they are not necessary to ensure officer safety or preserve evidence. *See id*. The same reasoning applies here and leads to the same conclusion. The privacy interests travelers have in the contents of their electronic devices are identical to those in *Riley*, and warrantless searches of electronic devices are not justified by the limited purposes of the border search exception, which are immigration and customs enforcement.

That government searches of electronic devices occur at the border does not alter the analysis. The border search exception to the Fourth Amendment's warrant

and probable cause requirements has always been subject to constitutional limits. As the Supreme Court held in *United States v. Ramsey*, "[t]he border-search exception is grounded in the recognized right of the sovereign to control, *subject to substantive limitations imposed by the Constitution*, who and what may enter the country." 431 U.S. 606, 620 (1977) (emphasis added). Thus, the border search exception—which permits warrantless and often suspicionless searches, *see United States v. Montoya de Hernandez*, 473 U.S. 531 (1985)—does not extend to electronic devices, and officers must obtain a warrant to search their contents.[10]

Two recent opinions bolster the conclusion that *Riley* supports the need for greater protections here. In *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018), the Fourth Circuit held that, following *Riley*, individualized suspicion is required for a forensic search of an electronic device seized at the border.[11] The court explained that "even before . . . *Riley*, there was a convincing case for categorizing forensic searches of digital devices as nonroutine" in light of the "sheer quantity of data stored" on them and the "uniquely sensitive nature of that information." *Id.* at

[10] Nothing in *Riley* forecloses applying its analysis to other categorical exceptions to the warrant requirement such as the border search exception. *See Riley*, 134 S. Ct. at 2484 (the search-incident-to-arrest exception is a "categorical rule"); *Ramsey*, 431 U.S. at 621 (the border search exception is "similar" to the search-incident-to-arrest exception).

[11] Because the issue was not raised on appeal, the court "ha[d] no occasion to consider application of the border exception to manual searches of electronic devices." *Kolsuz*, 890 F.3d at 141.

144–5. And "[a]fter *Riley*, we think it is clear that a forensic search of a digital phone must be treated as a nonroutine border search, requiring some form of individualized suspicion." *Id.* at 146. Because the court ultimately denied suppression on the basis of the good-faith exception to the exclusionary rule, it declined to decide what quantum of individualized suspicion is required for a forensic search of an electronic device at the border. But it recognized that "certain searches conducted under exceptions to the warrant requirement may require more than reasonable suspicion" and explicitly held open the question whether "the same is true of some nonroutine border searches." *Id.* at 147; *see also United States v. Vergara*, 884 F.3d 1309, 1313 (11th Cir. 2018) (J. Pryor, J., dissenting) (stating that, pursuant to the analysis in *Riley*, "a forensic search of a cell phone at the border requires a warrant supported by probable cause").[12]

In *Alasaad v. Nielsen*, No. 17-cv-11730, 2018 WL 2170323 (D. Mass. May 9, 2018), the court denied the government's motion to dismiss First and Fourth Amendment claims brought by 11 travelers whose electronic devices were searched at the U.S. border. The court explained that "*Riley* . . . indicate[s] that electronic device searches are, categorically, more intrusive than searches of one's

[12] The defendant in *Vergara* did not challenge the manual search of his phone, *see* 884 F.3d at 1312. The unpersuasive majority opinion in *Vergara*, which failed to adequately grapple with *Riley*, was followed in the Eleventh Circuit by *United States v. Touset*, where the panel again incorrectly held that warrantless—and indeed suspicionless—border device searches are permissible. *See* 890 F.3d 1227 (11th Cir. 2018).

person or effects. The ability to review travelers' cell phones allows officers to view 'nearly every aspect of their lives—from the mundane to the intimate.'" *Id.* at *20 (citations omitted). Thus, "[a]lthough Defendants may be correct that the border is different, the Supreme Court . . . ha[s] acknowledged that digital searches are different too since they 'implicate privacy concerns far beyond those implicated' in a typical container search." *Id.* at 2488–89. The court left for a later stage of the case the determination of what level of individualized suspicion is required for border searches of electronic devices.

a. Travelers Have Extraordinary Privacy Interests in the Digital Data Their Electronic Devices Contain.

Riley counsels that when it comes to warrantless searches of digital devices, courts must take serious account of the degree of the privacy invasion. *See Riley*, 134 S. Ct. at 2488–89.

A decade ago, a typical commercially available 80-gigabyte hard drive could carry data "roughly equivalent to forty million pages of text—about the amount of information contained in the books on one floor of a typical academic library." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005). Today's devices are even more capacious. Laptops for sale in 2018 can

store two terabytes,[13] the equivalent of more than 1.3 billion pages of text.[14] Even tablet computers can be purchased with up to a terabyte of storage.[15]

Smartphones also provide large storage capacities and can hold the equivalent of "millions of pages of text, thousands of pictures, or hundreds of videos." *Riley*, 134 S. Ct. at 2489. Moreover, the availability of cloud-based storage, email, and social media services can increase exponentially the functional capacity of a device.[16]

Not only do electronic devices contain or provide access to great quantities of data, they also contain a diverse array of information—much of it exceedingly sensitive. As the Supreme Court explained in *Riley*, cell phones are "minicomputers that . . . could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." 134 S. Ct. at 2489; *accord United States v. Cotterman*, 709 F.3d 952,

---

[13] *See* Apple, *Compare Mac models*, https://www.apple.com/mac/compare/ (last visited July 16, 2018).

[14] *See* LexisNexis, *How Many Pages in a Gigabyte?* (2007), http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf.

[15] *See* Microsoft, *Meet the New Surface Pro*, https://www.microsoft.com/en-us/surface/devices/surface-pro/overview (last visited July 16, 2018); Apple, *Compare iPad Models*, https://www.apple.com/ipad/compare/#ipad-pro-10-5,ipad (last visited July 16, 2018) (iPads available with up to one half terabyte (512 GB) of storage).

[16] *See, e.g.*, Google Drive, *Pricing Guide*, https://www.google.com/drive/pricing/ (last visited July 16, 2018) (offering up to 10 terabytes of paid cloud storage).

964 (9th Cir. 2013) (en banc). Many categories of information that courts have recognized as deserving of particularly stringent privacy protections can be contained on people's mobile devices, including Internet browsing history,[17] medical records,[18] historical cell phone location data,[19] email,[20] privileged communications,[21] and associational information.[22]

The data contained on mobile devices is also particularly sensitive because it does not represent merely isolated snapshots of a person's life, but can span years. Indeed, "[t]he sum of an individual's private life can be reconstructed through a

---

[17] *See Riley*, 134 S. Ct. at 2490 ("An Internet search and browsing history, for example . . . could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

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

[19] *See Carpenter*, 138 S. Ct. at 2222 (holding that historical cell phone location information is subject to the Fourth Amendment's warrant requirement given its sensitivity); *Riley*, 134 S. Ct. at 2490 ("Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.").

[20] *See United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) ("[E]mail requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve.").

[21] *See Jaffee v. Redmond*, 518 U.S. 1, 15 (1996) (psychotherapist-patient privilege); *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981) (attorney-client privilege); *Blau v. United States*, 340 U.S. 332, 333 (1951) (marital communications privilege).

[22] *See Riley*, 134 S. Ct. at 2490; *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958) ("[C]ompelled disclosure of affiliation with groups engaged in advocacy may constitute . . . a restraint on freedom of association . . . .").

thousand photographs labeled with dates, locations, and descriptions" or a "record of all [a person's] communications." *Riley*, 134 S. Ct. at 2489. Much of the private data that can be accessed in a search of a mobile device has no analogue in pre-digital searches because it never could have been carried with a person, or never existed at all. This includes deleted items that remain in digital storage unbeknownst to the device owner, historical location data, cloud-stored information, metadata about digital files created automatically by software on the device, and password-protected or encrypted information. *Riley*, 134 S. Ct. at 2490–91; *Cotterman*, 709 F.3d at 965.

Any search of a mobile device therefore implicates significant and unprecedented privacy interests. *Riley*, 134 S. Ct. at 2488–91; *see also Carpenter*, 138 S. Ct. at 2217–19.

A regime of suspicionless device searches also implicates First Amendment freedoms. In the closely-related context of customs searches of incoming international mail, the Supreme Court recognized that First Amendment-protected speech might be chilled by such searches. While the Court declined to invalidate the existing search regime, it notably did so because of regulations "flatly prohibit[ing], under all circumstances" customs officials from reading correspondence without a search warrant. *Ramsey*, 431 U.S. at 623. The Supreme Court explicitly left open the question of whether, "in the absence of the existing

statutory and regulatory protection," "the appropriate response [to a chill on speech] would be to apply the full panoply of Fourth Amendment requirements." *Id*. at 624 & n.18. Notably, the government recognizes no restriction on reading the vast quantities of correspondence and other personal information accessible on an electronic device seized at the border.

Border searches of electronic devices allow government agents to read and analyze all of the vast amount of data stored on a mobile device with little time and effort. *See generally Cotterman*, 709 F.3d 952. They thus reveal the "sum of an individual's private life," *Riley*, 134 S. Ct. at 2489, and "bear[] little resemblance" to searches of travelers' luggage, *id.* at 2485.

b. The Government's Interests Must Be Assessed in Light of the Narrow Purposes of the Border Search Exception.

Under the *Riley* balancing test, the government's interests are analyzed by considering whether warrantless searches of a category of property are "tethered" to the narrow purposes justifying the warrant exception. *See Riley*, 134 S. Ct. at 2485; *Kolsuz*, 890 F.3d at 143 ("[T]he scope of a warrant exception should be defined by its justifications."); *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"). Here, warrantless searches of electronic devices are not sufficiently tethered to the narrow purposes justifying the border search exception: immigration and customs enforcement. *See Montoya de*

Hernandez, 473 U.S. at 537 (authority to conduct suspicionless routine searches at the border is "in order to regulate the collection of duties and to prevent the introduction of contraband"); *Carroll v. United States*, 267 U.S. 132, 154 (1925) (travelers may be stopped at the border so as to identify themselves as "entitled to come in" and their belongings as "effects which may be lawfully brought in"); *Boyd v. United States*, 116 U.S. 616, 623 (1886) (discussing history of revenue acts allowing search and seizure of goods for "breach of the revenue laws, or concealed to avoid the duties payable on them"); *Cotterman*, 709 F.3d at 956 (emphasizing "narrow" scope of border search exception). The district court in this case, while declining to address the "difficult issues" raised by suspicionless border device searches, nonetheless recognized that allowing "unfettered access to information contained . . . [in] an individual's personal electronic devices" would "'untether'" the border search "rule from the justifications underlying it." App. 23.

As with the search-incident-to-arrest exception—justified by the limited goals of protecting officer safety and preventing the destruction of evidence—the border search exception may "strike[] the appropriate balance in the context of physical objects" such as luggage, but its underlying rationales do not have "much force with respect to digital content on cell phones" or other electronic devices. *Cf. Riley*, 134 S. Ct. at 2484. In other words, "even a search initiated at the border could become so attenuated from the rationale for the border search exception that

it no longer would fall under that exception." *Kolsuz*, 890 F.3d at 143. Border officers 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 officers enforce customs laws by searching travelers' luggage, vehicles, and, if necessary, their persons. *See, e.g.*, *United States v. Flores-Montano*, 541 U.S. 149, 151 (2004). As courts have recognized, "[d]etection of such contraband is the strongest historic rationale for the border-search exception." *United States v. Molina-Isidoro*, 884 F.3d 287, 295 (5th Cir. 2018) (Costa, J., specially concurring); *Alasaad v. Nielsen*, 2018 WL 2170323, at *18–*20 (discussing government interest in border searches as keeping out contraband); *see also Montoya de Hernandez*, 473 U.S. at 537–38 (same). Yet, in most circumstances, "this detection-of-contraband justification would not seem to apply to an electronic search of a cell phone or computer," *Molina-Isidoro*, 884 F.3d at 295 (Costa, J., specially concurring), because "cell phones do not contain the physical contraband that border searches traditionally have prevented from crossing the border," *Vergara*, 884 F.3d at 1317 (J. Pryor, J., dissenting). The Supreme Court has long emphasized the limited nature of customs searches. *See Boyd*, 116 U.S. at 623 ("The search for and seizure of stolen or forfeited goods, or 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.").

While some digital content, such as the suspected child pornography at issue in this case, may be considered "digital contraband" to be interdicted at the border, *cf. United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376–77 (1971), that characterization would not justify a categorical rule permitting warrantless searches of any and all electronic devices. Unlike physical contraband, digital contraband can easily be transported across borders via the Internet, so individuals need not transport it physically across the border, nor can a border search succeed in keeping such digital data definitively out of the country. *See Vergara*, 884 F.3d at 1317 (J. Pryor, J., dissenting) ("[C]ell phone searches are ill suited to prevent the type of contraband that may be present on a cell phone from entering into the United States. Unlike physical contraband, electronic contraband is borderless and can be accessed and viewed in the United States without ever having crossed a physical border."); *accord Alasaad*, 2018 WL 2170323, at *19. Additionally, digital contraband that is located solely in the cloud cannot be considered to be crossing the border and therefore subject to a border search. *See Riley*, 134 S. Ct. at 2491 (the search-incident-to-arrest exception "may not be stretched to cover a search of files accessed remotely" because that "would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search

a house").[23] Thus, the government cannot demonstrate that any digital contraband that might be physically resident on travelers' devices is a significant or "prevalent" problem (in the words of the *Riley* Court) *at the border* that justifies or necessitates a *categorical rule* permitting warrantless border searches of electronic devices for every traveler entering or exiting the country. *Cf. Riley*, 134 S. Ct. at 2485–86 (noting insufficient evidence that warrantless searches of arrestees' cell phones would meaningfully protect officer safety or prevent destruction of evidence and that, in any event, such possibilities do "not justify dispensing with the warrant requirement across the board").

Of course, where border officers have probable cause to believe contraband data is stored on a device, it is feasible to go through the process of securing a search warrant—as the government did for the later forensic searches of Mr. Wanjiku's devices. App. 19. And in rare instances where there is truly no time to go to a judge, the exigent circumstances exception may apply. *See Carpenter*, 138 S. Ct. at 2223; *Riley*, 134 S. Ct. at 2486.

Even assuming that warrantless device searches at the border might sometimes advance the government's goals of immigration and customs enforcement, the extraordinary privacy interests travelers have in their electronic devices outweigh any governmental interests. *See Kolsuz*, 890 F.3d at 145-46. As a

[23] Unlike CBP's 2018 policy, ICE's 2009 policy does not prohibit border searches of cloud content.

result, the Fourth Amendment requires that border officers must obtain a warrant before searching electronic devices.

ii. Under the Supreme Court's Pre-*Riley* Border Cases, Warrantless Searches of Electronic Devices are Unreasonable.

Even before the Supreme Court's ruling in *Riley*, preexisting border search precedent provided a parallel justification for requiring a warrant based on probable cause for border searches of electronic devices. *See Kolsuz*, 890 F.3d at 144 ("[E]ven before . . . *Riley*, there was a convincing case for categorizing forensic searches of digital devices as nonroutine."). This body of case law on border searches bolsters the *Riley* analysis to dictate that warrantless searches of electronic devices are constitutionally unreasonable.

The Supreme Court has held that the scope of the border search exception to the warrant requirement is not unlimited, and that "[t]he Fourth Amendment commands that searches and seizures [at the border] be reasonable." *Montoya de Hernandez*, 473 U.S. at 537. As in other contexts, "[w]hat is reasonable depends upon all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself." *Id.* For example, the Court has 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.'" *Flores-Montano*, 541 U.S. at 154 n.2 (quoting *Ramsey*, 431 U.S. at 618 n.13).

Warrantless border searches of devices cross the line that the Supreme Court contemplated and violate the Fourth Amendment's reasonableness requirement.

First, as explained above, device searches intrude upon the substantial privacy interests that travelers have in their electronic devices. *Ramsey* underscores the scale of those interests, even at the border. That case distinguished the search of a vessel or container from the search of a house—which, the Court noted, required a warrant even before the ratification of the Constitution, 431 U.S. at 617—and it observed that "a port of entry is not a traveler's home." *Id.* at 618. Yet a search of a cell phone "would typically expose to the government far *more* than the most exhaustive search of a house." *See Riley*, 134 S. Ct. at 2491 (emphasis in original).

Second, border device searches raise grave First Amendment concerns that affect the reasonableness analysis. In *Ramsey*, the Court left open the possibility that where First Amendment rights are implicated by a border search, the "full panoply" of Fourth Amendment protections—*i.e.*, a warrant requirement—might apply. 431 U.S. at 623–24 & n.18.

Third, device searches at the border are often conducted in a "particularly offensive manner." *See Flores-Montano*, 541 U.S. at 154 n.2. As Mr. Wanjiku's

experience demonstrates, officers can and do use threats of device confiscation to extract passcodes from travelers, search the devices' content for lengthy periods, and retain the contents of the devices. *See* App. 16–19.

Requiring a warrant for border device searches is both feasible and necessary to satisfy the Fourth Amendment's reasonableness requirement. *See Riley*, 134 S. Ct. at 2493 ("Recent technological advances . . . have . . . made the process of obtaining a warrant itself more efficient."). Indeed, the Supreme Court has contemplated a warrant process at the border. *See Ramsey*, 431 U.S. at 623–24; *Montoya de Hernandez*, 473 U.S. at 547 & n.13.[24]

B. The Warrant Requirement Should Apply to Border Device Searches Irrespective of Search Method Used

In this case, Mr. Wanjiku was subject to manual and forensic searches of his phone absent a warrant. App. 16–19. Although most cases requiring individualized

[24] Many of the federal district court cases deciding to the contrary preceded *Riley*. *See United States v. Hampe*, No. 07-3-B-W, 2007 WL 1192365 (D. Me. Apr. 18, 2007); *House v. Napolitano*, No. 11-10852-DJC, 2012 WL 1038816 (D. Mass. Mar. 28, 2012). Others, from the Ninth Circuit, are bound by *Cotterman*, which itself preceded *Riley*. *See United States v. Mendez*, No. CR-16-00181-001-TUC-JGZ (JR), 2017 WL 928460 (D. Ariz. Mar. 9, 2017); *United States v. Cano*, 222 F. Supp. 3d 876 (S.D. Cal. 2016); *United States v. Ramos*, 190 F. Supp. 3d 992 (S.D. Cal. 2016); *United States v. Lopez*, No. 13-CR-2092 WQH, 2016 WL 7370030 (S.D. Cal. Dec. 20, 2016); *United States v. Hernandez*, No. 15-CR-2613-GPC, 2016 WL 471943 (S.D. Cal. Feb. 8, 2016). Others are unpersuasive for the reasons set forth above. *See United States v. Feiten*, No. 15-20631, 2016 WL 894452 (E.D. Mich. Mar. 9, 2016); *Abidor v. Johnson*, No. 10-CV-4059 (ERK), 2016 WL 3102017 (E.D.N.Y. June 2, 2016); *United States v. Blue*, No. 1-14-CR-244-SCJ, 2015 WL 1519159 (N.D. Ga. Apr. 1, 2015); *United States v. Saboonchi*, 48 F. Supp. 3d 815 (D. Md. 2014).

suspicion for searches of electronic devices at the border have addressed forensic searches, *see, e.g.*, *Kolsuz*, 890 F.3d at 142; *Cotterman*, 709 F.3d at 961, there is no valid distinction between manual and forensic searches for Fourth Amendment purposes because both severely harm privacy by accessing essentially the same trove of highly personal information. Indeed, the facts of this and other cases "demonstrate the level of intrusiveness a manual device search can entail." *Alasaad*, 2018 WL 2170323, at *20.

In the case of manual searches, the existence of cloud-based services on smartphones—including email, social media, financial, or health services—means that even a brief search of a mobile device could allow a government agent access to a vast trove of private information.[25] Even without accessing cloud-stored data, an officer without specialized training or equipment can conduct keyword searches using the device's built-in search function, thereby accessing virtually the same information as a forensic search.[26] Manual searches can access emails, voicemails, text messages, call logs, contact lists, photographs, videos, calendar entries,

[25] In July 2017, CBP publicly announced that its officers are not supposed to access cloud-stored data during border searches of electronic devices. The searches at issue in this case took place in 2015, prior to this public statement by CBP. *See* 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.

[26] Apple's iPhone currently has a search function for the entire phone that pulls content based on keywords. Apple, *Use Search on Your iPhone, iPad, or iPod Touch*, https://support.apple.com/en-us/HT201285 (last visited July 16, 2018).

shopping lists, personal notes, and web browsing history. Even a history of a traveler's physical location may be uncovered through a manual search: for example, 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.[27] As the cost of storage drops and technology advances, digital devices will hold ever greater amounts of personal information and feature increasingly powerful search capabilities. Thus, manual searches will reveal ever more personal information, making the distinction between them and forensic searches meaningless. For these reasons, Fourth Amendment protections should apply no less robustly to manual searches of electronic devices than to forensic searches of electronic devices.

Forensic or "advanced" searches, like the so-called "forensic 'preview'" searches in this case, which required specialized equipment or software, *see* App. 17–19, are likewise highly invasive.[28] The forensic search tools used by the government can extract and analyze tremendous quantities of data. Here, for example, an agent employed "enCase" software to search Mr. Wanjiku's external hard drive. App. 18. In another case, the same software was employed "to export

[27] *See* Google, *Google Maps Help*, https://support.google.com/maps/answer/6258979?co=GENIE.Platform%3DDesktop&hl=en (last visited July 16, 2018).

[28] This Court should not give any significance to the government's use of the word "preview"—as the district court in this case noted, the government at trial acknowledged "that the same software the agents used to preview the hard drive was also used for the full forensic examination." App. 19. The "full forensic searches" did not uncover any additional evidence in this case. App. 20.

six Microsoft Outlook email containers," which can each contain thousands of email messages, "8,184 Microsoft Excel spreadsheets, 11,315 Adobe PDF files, 2,062 Microsoft Word files, and 879 Microsoft PowerPoint files," as well as "approximately 24,900 .jpg [picture] files," from a laptop. *United States v. Kim*, 103 F. Supp. 3d 32, 40–41 & n.3 (D.D.C. 2015). Mr. Wanjiku's cell phone was also subject to a search using specialized software that could "extract data and create an HTML report." App. 18. Although the agents chose to confine their warrantless search of Mr. Wanjiku's cell phone to images and videos, they could have done a more comprehensive search of "unallocated space," including deleted items, as well as text messages, emails, and other data on the phone. *See* App. 18. Any time a device seized at the border remains in government custody, it is potentially subject to a forensic search, as took place with all three of Mr. Wanjiku's devices.

Before *Riley*, the Ninth Circuit in *Cotterman* required reasonable suspicion for a forensic search and no suspicion for a manual search. 709 F.3d at 967–68. But that distinction has become legally and technologically untenable, as this case demonstrates, given that each of the search methods used by the government agents revealed extraordinarily private information, regardless of whether the search was classified as manual or a particular type of forensic search. Given the increasing volume and detail of personal information in electronic devices, and the

growing ease of manually navigating them, manual searches are extraordinarily invasive of travelers' privacy. Indeed, the unlawful warrantless cell phone searches in *Riley* were manual. *See* 134 S. Ct. at 2480–81, 2493; *see also Kim*, 103 F. Supp. 3d at 55 (the reasonableness of a border device search does not "turn on the application of an undefined term like 'forensic'").

CONCLUSION

For the foregoing reasons, this Court should hold that federal agents violated the Fourth Amendment by searching Mr. Wanjiku's electronic devices without a warrant based on probable cause.

Dated: July 18, 2018

Respectfully submitted,

/s/Esha Bhandari

Adam Schwartz
Sophia Cope
Aaron Mackey
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333
Fax: (415) 436-9993
adam@eff.org
sophia@eff.org
amackey@eff.org

Rebecca Glenberg
ROGER BALDWIN FOUNDATION OF ACLU, INC.
180 N. Michigan Ave., Suite 2300
Chicago, IL 60601
Phone: (312) 201-9740
rglenberg@aclu-il.org

Esha Bhandari
Nathan Freed Wessler
Hugh Handeyside
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., Floor 18
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2583
ebhandari@aclu.org
nwessler@aclu.org
hhandeyside@aclu.org

Counsel for amici curiae

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7) and Federal Rule of Appellate Procedure 29(a)(5) because it contains 6,499 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f).
2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) because this brief was prepared on a computer, using Microsoft Word, in Times New Roman (proportionally spaced) typeface, 14-point type, double-spaced, with 14-point single-spaced footnotes.

Dated: July 18, 2018

/s/Esha Bhandari
Esha Bhandari

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 18th day of July, 2018, the foregoing Brief of *Amici Curiae* American Civil Liberties Union, ACLU of Illinois, and Electronic Frontier Foundation was filed electronically through the Court's CM/ECF system. Notice of this filing will be sent by email to all parties by operation of the Court's electronic filing system.

/s/Esha Bhandari
Esha Bhandari