No. 16-4687

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA

Plaintiff–Appellee,

v.

HAMZA KOLSUZ

Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE EASTERNDISTRICT OF VIRGINIA, ALEXANDRIA DIVISION

BRIEF OF AMICI CURIAE

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is not required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. _____ Caption: _____

Pursuant to FRAP 26.1 and Local Rule 26.1,

_____
(name of party/amicus)

_____

who is _____, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? YES

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(a)(2)(B))? YES NO
If yes, identify entity and nature of interest:

5. Is party a trade as

TABLE OF CONTENTS

TABLE OF AUTHORITIES iv

INTEREST OF AMICI CURIAE 1

SUMMARY OF ARGUMENT 2

ARGUMENT 4

I. This Court Should Decide the Fourth Amendment Question Regardless of Whether Suppression Is Warranted 4

A. Border Searches of Electronic Devices Are Increasing Rapidly, With a Fivefold Increase in 2016 4

B.

United States v. Flores-Montano, 541 U.S. 149 (2004) 19, 20

United States v. Hassanshahi, 75 F. Supp. 3d 101 (D.D.C. 2014) 9

United States v. Ickes, 393 F.3d 501 (4th Cir. 2005) 18, 26

United States v. Jones, 132 S. Ct. 945 (2012) 16

United States v. Kim, 103 F. Supp. 3d 32 (D.D.C. 2015) ..... passim

United States v. Lahiri, No. 08-20089, 2010 WL 259041 (E.D. Mich. Jan. 20, 2010) 22, 25

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) 16

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

United States v. Ramsey, 431 U.S. 606 (1977) ..... passim

United States v. Robinson, 414 U.S. 218 (1973) 19

United States v. Saboonchi, 990 F. Supp. 2d 536 (D. Md. 2014) 9

United States v. Vega-Barvo, 729 F.2d 1341 (11th Cir. 1984) 26

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) 17, 24

United States v. Whitted, 541 F.3d 480 (3d Cir. 2008) 25, 27

United States v. Yang, 286 F.3d 940 (7th Cir. 2002) 27

Upjohn Co. v. United States, 449 U.S. 383 (1981) 11

Wyoming v. Houghton, 526 U.S. 295 (1999) 20

Other Authorities

Aaron Smith, Pew Research Ctr., U.S. Smartphone Use in 2015, Chapter Three: A “Week in the Life” Analysis of Smartphone Users (2015) 8

Apple, Compare Mac models 10

U.S. Customs and Border Protection, Border Search of Electronic Devices Containing Information, Directive No. 3340-049 (Aug. 20, 2009) 6, 7

U.S. Dep't of Homeland Sec., Civil Rights/Civil Liberties Impact Assessment: Border Searches of Electronic Devices (2011) 41

INTEREST OF AMICI CURIAE [1]

SUMMARY OF ARGUMENT

This case presents an important question about the extent of Fourth Amendment privacy rights in the digital age, where the use of mobile devices is widespread. The government's assertion of authority to search such devices without any individualized suspicion when an individual is crossing the border whether entering or leaving the United States creates an end-run around Fourth Amendment protections that would otherwise apply to the voluminous and intimate information contained in those devices, and is not justified by the rationale permitting routine border searches.

Hundreds of millions of people cross the United States' borders every year for school, business, pleasure, and family obligations. A large numbers of those travelers carry laptops, smartphones, and other portable electronic devices that, aT la vromation co5(ha)3.6(s)8.4(p v)8.3(1(vi)8.5(c)3.6(e)12.1(s3-8.8(c)3.5(r))3.5(r)3.7(r

ARGUMENT

I. This Court Should Decide the Fourth Amendment Question Regardless of Whether Suppression Is Warranted

This Court should address the Fourth Amendment question of what level of suspicion is required bef

searched. See Gillian Flaccus, Electronic Media Searches at Border Crossings Raise Worry, AP, Feb. 18, 2017, http://apne.ws/2mQFeUg [hereinafter "Flaccus"] (identifying 23,877 electronic media searches in 2016). The Department of Homeland Security has justified its practice of searching electronic devices in part by noting "how infrequent[ly such] searches are conducted,"[5] but border searches of electronic devices were up fivefold in 2016. See Flaccus (noting that electronic media searches rose from 4,764 in 2015 to 23,877 in 2016).

Searches of electronic devices have already made news this year. On January 31, 2017, U.S. Customs and Border Protection ("CBP") officers reportedly detained a U.S.-born engineer working at NASA's Jet Propulsion Laboratory until he agreed to hand over the confidential PIN code necessary to access his employer-issued smartphone.[6] Another U.S. citizen was stopped at Los Angeles International Airport when attempting to exit the country and recalls being repeatedly pressured to unlock his smartphone so agents

border." ICE Policy § 8.6(1). Under CBP policy, an officer or agent "may be subject" to the requirement that he "seek advice" from counsel before accessing "legal material," but CBP does not require officials to seek such advice. CBP Policy § 5.2.1.

These policies have been reaffirmed in recent years, both in policy documents, see, e.g., DHS CR/CL Impact Assessment ("[W]e are not recommending that officers demonstrate reasonable suspicion for the device search . . . ."), and in litigation filings.[10] The effect of these 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 electronic devices in their possession.[11]

Use of mobile, or portable, 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); Riley, 134 S. Ct. at 2490 (90 percent prevalence in 2014). Today, 77 percent of American adults own a smartphone, and rates of smartphone ownership are higher

[10] See, e.g., J.A. 45–50; see also, e.g., Br. of Appellee, United States v. Vergara, No. 16-15059, 2017 WL 360182, at *14–17 (11th Cir. Jan. 23, 2017).

[11] The government's claimed authority to conduct suspicionless searches of electronic devices seized at the border applies to travelers entering and departing the country. See CBP Policy § 1; ICE Policy § 1.1.

among younger Americans[12]—who travel internationally at increasingly high rates.[13] People rely on these devices for communication (via text messages, calls, email, and social networking), navigation, entertainment, news, photography, and a multitude of other functions.[14] In addition, more than ten 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.[15] 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.[16]

People consistently carry these devices with them, including when they travel. Indeed, "[a]ccording to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12 percent

---

[12] Pew Mobile Fact Sheet.

[13] 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/.

[14] 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/.

[15] Pew Mobile Fact Sheet.

[16] Deloitte, Digital Democracy Survey 5 (9th ed. 2015), http://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-DDS_Executive_Summary_Report_Final_2015-20.pdf.

terabytes,[17] the equivalent of more than 1.2 billion pages of text.[18] Even tablet computers can be purchased with a terabyte of storage.[19]

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 exponentially increase the functional capacity of a device.[20]

Not only do portable 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*, smartphones 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; see also *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (en banc) ("Laptop computers, iPads and the like are

---

[17] See Apple, Compare Mac models, https://www.apple.com/mac/compare/ (last visited March 19, 2017).

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

[19] See Microsoft, Surface Pro 4, https://www.microsoft.com/en-us/surface/devices/surface-pro-4/overview (last visited Mar. 19, 2017).

[20] See, e.g., Google, Drive Help, https://support.google.com/drive/answer/2375123 (last visited Mar. 19, 2017) (offering up to 30 terabytes of paid cloud storage).

simultaneously offices and personal diaries. They contain financial records, confidential business documents, medical records and private emails. 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,[21] medical records,[22] historical cell phone location data,[23] email,[24] privileged communications,[25] and associational information.[26]

---

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

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

[23] See 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.").

[24] 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.").

[25] 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).

[26] Riley, 134 S. Ct at 2490 ("Mobile application software on a cell phone, or

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 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 would have 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 serious privacy interests. *Riley*, 134 S. Ct. at 2488–91. Furthermore, a regime of suspicionless device searches 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. *United States v.*

Ramsey, 431 U.S. 606, 623 (1977). 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 similar restriction on reading the information accessible on an electronic device seized at the border, even though the chill on First Amendment rights may be even greater because of the quantity and quality of information contained.

These privacy and First Amendment concerns are implicated regardless of whether border officials do a "cursory" or "manual" search of a device, or a so-called "forensic" search. In the case of cursory 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. An agent may be able to click on an email application and read thousands of emails stored on remote servers, or do the same with a health application and see years' worth of data about heart rates, reproductive cycles, and more. Even without accessing cloud-stored data, an officer without specialized training or equipment can conduct extensive keyword searches using the device's built-in search function, thereby achieving

The forensic search tools used by the government can extract and analyze tremendous quantities of data.[30] In one recent case, for example, an agent "employed a software program called EnCase . . . to export 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 & n.3 (D.D.C. 2015). In the instant case, the government employed a Cellebrite Physical Analyzer, "a tool that extracts data from electronic devices, and conducted an advanced logical file system extraction." Jan. App'x 196. This resulted in enough data to "fill 896 printed pages," which the district court rightly concluded is "such an immense amount of disparate personal information" that it "allows the government to reconstruct 'an individual's private life.'" J. App'x 209 (quoting Riley ,

United States, 533 U.S. 27, 34 (2001); see also United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010) ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and

States v. Feiten, No. 15-20631, 2016 WL 894452, at *4 (E.D. Mich. Mar. 9, 2016)(holding the opposite). This Court should take up the mantle of ensuring that the Fourth Amendment is not allowed to atrophy in the face of rapid technological change.

Guidance from this Court is also important to ensure that government agents do not take the wrong lessons from prior holdings of this Court that do not apply here. In particular, United States v. Ickes, 393 F.3d 501 (4th Cir. 2005), should not be read to justify suspicionless border searches of electronic devices. Like Cotterman, Ickes was decided before Riley's privacy-protective framework for device searches. The defendant's only argument in Ickes was about the need for a heightened Fourth Amendment standard when "expressive materials" are searched. Ickes, 393 F.3d at 507. The acute privacy harm of exhaustive searches of digital devices was not at issue, nor did the Court fully grapple with the sheer amount and sensitivity of the information contained in a mobile device. This Court should make clear that neither the facts nor reasoning of Ickes justify suspicionless border searches of electronic devices.

II. Searches of Electronic Devices Seized at the Border Require a Warrant or Probable Cause

As the Supreme Court has repeatedly declared, "'searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically

established and well-delineated exceptions." *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). Among those exceptions are search incident to arrest,[31] search pursuant to exigent circumstances,[32] vehicular search,[33] and border search.[34] But none of these exceptions apply automatically upon invocation; rather, they must remain "[]tether[ed]" to "the justifications underlying the . . . exception." *Gant*, 556 U.S. at 343 (holding that the search

Hernandez, 473 U.S. at 540, the government's interest is limited to determining the admissibility of individuals and preventing the transport of contraband.

On the other side of the balance, the individual's privacy interest in the contents of a smartphone or laptop is extraordinarily strong. See Riley, 134 S. Ct at 2491UiS3.7(d27.(u3 -2.29B6([0.ex2(ily) c(e)12.1)3.6e((d)-8.3248 te)12.)3.6(or)3.7s or

others, and the right to dispose of property. The initial copying constitutes a seizure for which a warrant is required, and as long as the government retains the copy, the intrusion on Fou

cannot be said to transport across the border digital data that is not stored on their device but merely accessible through the internet. The same is true for deleted data that can be retrieved during a forensic search. Br. of Appellee, United States v. Vergara, No. 16-15059, 2017 WL 360182, at *27 (11th Cir. Jan 23, 2017) (government argument in pending Eleventh Circuit case that border searches are justified because they "afford[] travelers ample opportunity to limit the items that may be subjected to a search" (emphasis added)).

And in cases like this one involving forensic searches of cell phone contents "the immediate national security concerns [are] somewhat attenuated." Kim, 103 F. Supp. 3d at 56–57. Forensic searches occur days or weeks after the border crossing, and can continue for long periods of time. See, e.g., Cotterman, 709 F.3d at 967 ("[In a forensic search,] agents will mine every last piece of data on [travelers'] devices [and] deprive them of their most personal property for days (or perhaps weeks or even months, depending on how long the search) . . ."); Kim, 103 F. Supp. 3d at 42 (quoting government agent's statement that the "identification and extraction process . . . may take weeks or months"). Though the government retains an interest in interdicting contraband and ensuring border

judge. Riley, 134 S. Ct at 2493 ("Recent technological advances similar to those discussed here have, in addition, made the process of obtaining a warrant itself more efficient.") The search in this case "'did not possess the characteristics of a border search or other regular inspection procedures'" but "'more resembled the common nonborder search based on individualized suspicion, which must be prefaced by the usual warrant and probable cause standards.'" Kim, 103 F. Supp. 3d at 58 (quoting

officers to nonetheless have probable cause). A probable cause threshold will help limit the massive privacy intrusion inflicted by device searches. *See Laich*, 2010 WL 259041, at *4. This will be particularly true as the search capabilities available to the government become more powerful and efficient. "It is little comfort to assume that the government—for now—does not have the time or resources to seize and search the millions of devices that accompany the millions of travelers who cross our borders. It is the potential unfettered dragnet effect that is troublesome." *Cotterman*, 709 F.3d at 966.

III. At an Absolute Minimum, Searches of Electronic Devices Seized at the Border Require Reasonable Suspicion Because They Are Non-Routine.

Although the Supreme Court has found that the government has broad powers to conduct searches at the border, *see Ramsey*, 431 U.S. at 616, it has also recognized that non-routine border searches require at least reasonable suspicion of wrongdoing, *Montoya de Hernandez*, 473 U.S. at 541. When deciding whether a search is non-routine, a court "must examine the degree to which it intrudes on a traveler's privacy." United States v. Whitted, 541 F.3d 480, 485 (3d Cir. 2008) (requiring reasonable suspicion for search of passenger cabin of a vessel); *accord* United States v. Braks, 842 F.2d 509, 511 (1st Cir. 1988) ("[T]he determining factor in assessing whether a search is routine or non-routine is "[t]he degree of invasiveness or intrusiveness"); United States v. Vega-Barvo, 729 F.2d 1341, 1346 (11th Cir.

associated with private dwelling areas than luggage and other effects, and should be treated accordingly. Cf. Whitted, 541 F.3d at 1088 (search of passenger cabin of a vessel requires reasonable suspicion); United States v. Alfonso, 759 F.2d 728, 738 (9th Cir. 1985) (finding that a border search of the private living quarters on a ship "should require something more than naked suspicion").

Second

347 (1957) ("The seizure of the entire contents of the house and its removal some two hundred miles away to the F.B.I. offices for the purpose of examination are beyond the sanction of any of our cases."). Because device searches can indiscriminately lay bare the entire contents of an electronic device, as well as any data the user has stored in a cloud-based service that can be accessed via the device, without limits on the search's duration, subject matter, or scope, such searches are particularly offensive. Thus, while searches of electronic devices at the border require a warrant or probable cause for the reasons described above, see *supra*, they also require at least reasonable suspicion as non-routine border searches.

CONCLUSION

This Court should hold that because searches of electronic devices seized at the border infringe deeply on privacy interests, such searches should only be permitted pursuant to a warrant or, at a minimum, probable cause.

March 20, 2017

Respectfully submitted,

/s/ Hope R. Amezquita

Hope R. Amezquita
American Civil Liberties Union Foundation of Virginia, Inc.
701 E. Franklin Street, Suite 1412
Richmond, VA 23219
Phone: (804) 644-8080
Fax: (804) 649-2733
hamezquita@acluva.org

Esha Bhandari
Nathan Freed Wessler
Vera Eidelman*
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ebhandari@aclu.org

David R. Rocah
American Civil Liberties Union
Foundation of Maryland
3600 Clipper Mill Road, Suite 350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
rocah@aclu-md.org

Susan K. Dunn
American Civil Liberties Union
Foundation of South Carolina
P.O. Box 20998
Charleston, SC 29413
Phone: (843) 282-7953
sdunn@aclusc.org

Irena Como
ACLU of North
Carolina Legal
Foundation, Inc.
P.O. Box 28004
Raleigh, NC 27611
Phone: (919) 834-3466
Fax: (866) 511-1344
icomo@aclunc.org

Jamie Lynn Crofts
ACLU of West Virginia
Foundation
P.O. Box 3952
Charleston, WV 25339
Phone: (304) 345-9246
Fax: (304) 345-0207
jcrofts@acluwv.org

*Admitted to the State Bar of California

CERTIFICATE OF COMPLIANCE

1. This brief complies with type-volume limits because, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f), it

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 20th day of March, 2017, the foregoing Brief of Amici Curiae American Civil Liberties Union, et al., 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/ Hope Amezquita

Hope Amezquita