

# New York Supreme Court

Appellate Division – Second Department

---

PEOPLE OF THE STATE OF NEW YORK,  
*Appellee,*

-against-

THOMAS E. PERKINS,  
*Defendant-Appellant.*

---

**BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION,  
ELECTRONIC FRONTIER FOUNDATION, AND NEW YORK CIVIL  
LIBERTIES UNION IN SUPPORT OF DEFENDANT-APPELLANT**

Adam Schwartz  
Sophia Cope  
Aaron Mackey  
ELECTRONIC  
FRONTIER  
FOUNDATION  
815 Eddy Street  
San Francisco, CA 94109  
(415) 436-9333 (phone)  
(415) 436-9993 (fax)

Esha Bhandari  
Nathan Freed Wessler  
Hugh Handeyside  
AMERICAN CIVIL  
LIBERTIES UNION  
FOUNDATION  
125 Broad Street,  
18th Floor  
New York, NY 10004  
(212) 549-2500 (phone)  
(212) 549-2583 (fax)

Christopher Dunn  
Aadhithi Padmanabhan  
NEW YORK CIVIL  
LIBERTIES UNION  
FOUNDATION  
125 Broad Street,  
19th Floor  
(212) 607-3300 (phone)  
(212) 607-3318 (fax)

Dated: May 15, 2018  
New York, N.Y.

## TABLE OF CONTENTS

TABLE OF AUTHORITIES .....	ii
INTEREST OF <i>AMICI CURIAE</i> .....	1
SUMMARY OF ARGUMENT .....	2
ARGUMENT .....	5
I. Border Searches of Electronic Devices Are Increasing Rapidly and Affect Large Numbers of Travelers.....	5
II. Warrantless, Suspicionless Searches of Electronic Devices at the Border Violate the Fourth Amendment.....	9
A. Under the Fourth Amendment, a Warrant is Required to Search the Contents of an Electronic Devices at the Border. ....	10
i. The Supreme Court’s Analysis in <i>Riley v. California</i> Dictates That a Warrant Is Required.....	10
a. Travelers Have Extraordinary Privacy Interests in the Digital Data Their Electronic Devices Contain. ....	14
b. The Government’s Interests Must Be Assessed in Light of the Narrow Purposes of the Border Search Exception. ....	18
ii. Under the Supreme Court’s Pre- <i>Riley</i> Border Cases, Warrantless Searches of Electronic Devices are Unreasonable.....	22
B. The Warrant Requirement Should Apply to Border Device Searches Irrespective of Search Method Used .....	25
CONCLUSION .....	29
CERTIFICATION OF COMPLIANCE .....	30

## TABLE OF AUTHORITIES

### Cases

<i>Abidor v. Johnson</i> , No. 10-CV-4059 (ERK), 2016 WL 3102017 (E.D.N.Y. June 2, 2016).....	25
<i>Alasaad v. Nielsen</i> , No. 17-cv-11730, 2018 WL 2170323 (D. Mass. May 9, 2018).....	13, 19, 21, 26
<i>Blau v. United States</i> , 340 U.S. 332 (1951).....	16
<i>Boyd v. United States</i> , 116 U.S. 616 (1886) .....	18, 20
<i>Carroll v. United States</i> , 267 U.S. 132 (1925) .....	18
<i>Ferguson v. Charleston</i> , 532 U.S. 67 (2001).....	15
<i>Florida v. Royer</i> , 460 U.S. 491 (1983) .....	18
<i>Hassanshahi</i> , 75 F. Supp. 3d 101 (D.D.C. 2014) .....	9
<i>House v. Napolitano</i> , No. 11-10852-DJC, 2012 WL 1038816 (D. Mass. Mar. 28, 2012) .....	25
<i>Jaffee v. Redmond</i> , 518 U.S. 1 (1996) .....	16
<i>NAACP v. Alabama ex rel. Patterson</i> , 357 U.S. 449 (1958).....	16
<i>People v. Weaver</i> , 12 N.Y. 3d 433 (2009).....	4
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014) .....	passim
<i>United States v. Blue</i> , No. 1-14-CR-244-SCJ, 2015 WL 1519159 (N.D. Ga. Apr. 1, 2015).....	25
<i>United States v. Cano</i> , 222 F. Supp. 3d 876 (S.D. Cal. 2016).....	25
<i>United States v. Cotterman</i> , 709 F.3d 952 (9th Cir. 2013).....	passim
<i>United States v. Feiten</i> , No. 15-20631, 2016 WL 894452 (E.D. Mich. Mar. 9, 2016).....	25
<i>United States v. Flores-Montano</i> , 541 U.S. 149 (2004) .....	19, 23, 24
<i>United States v. Hampe</i> , No. 07-3-B-W, 2007 WL 1192365 (D. Me. Apr. 18, 2007).....	25
<i>United States v. Hernandez</i> , No. 15-CR-2613-GPC, 2016 WL 471943 (S.D. Cal. Feb. 8, 2016).....	25
<i>United States v. Kim</i> , 103 F. Supp. 3d 32 (D.D.C. 2015).....	28, 29

<i>United States v. Kolsuz</i> , No. 16-4687, 2018 WL 2122085 (4th Cir. May 9, 2018).....	passim
<i>United States v. Lopez</i> , No. 13-CR-2092 WQH, 2016 WL 7370030 (S.D. Cal. Dec. 20, 2016).....	25
<i>United States v. Mendez</i> , No. CR-16-00181-001-TUC-JGZ (JR), 2017 WL 928460 (D. Ariz. Mar. 9, 2017).....	25
<i>United States v. Molina-Isidoro</i> , 267 F. Supp. 3d 900 (W.D. Tex. 2016) .....	25
<i>United States v. Molina-Isidoro</i> , 884 F.3d 287 (5th Cir. 2018) .....	19
<i>United States v. Montoya de Hernandez</i> , 473 U.S. 531 (1985).....	passim
<i>United States v. Ramos</i> , 190 F. Supp. 3d 992 (S.D. Cal. 2016) .....	25
<i>United States v. Ramsey</i> , 431 U.S. 606 (1977) .....	passim
<i>United States v. Saboonchi</i> , 48 F. Supp. 3d 815 (D. Md. 2014).....	25
<i>United States v. Saboonchi</i> , 990 F. Supp. 2d 536 (D. Md. 2014).....	9
<i>United States v. Thirty-Seven Photographs</i> , 402 U.S. 363 (1971) .....	20
<i>United States v. Vergara</i> , 884 F.3d 1309 (11th Cir. 2018).....	13, 20, 21
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010) .....	16
<i>Upjohn Co. v. United States</i> , 449 U.S. 383 (1981).....	16

**Other Authorities**

Aaron Smith, Pew Research Ctr., <i>U.S. Smartphone Use in 2015, Chapter Three: A “Week in the Life” Analysis of Smartphone Users</i> (2015) .....	8
Apple, <i>Compare iPad Models</i> .....	14
Apple, <i>Compare Mac models</i> .....	14
Apple, <i>Use Search on Your iPhone, iPad, or iPod Touch</i> .....	26
Deloitte, <i>Digital Democracy Survey</i> (9th ed. 2015) .....	8
E.D. Cauchi, <i>Border Patrol Says It’s Barred From Searching Cloud Data on Phones</i> , NBC News (July 12, 2017) .....	26
Google, <i>Google Maps Help</i> .....	27
Google, <i>Pricing Guide</i> .....	15
LexisNexis, <i>How Many Pages in a Gigabyte</i> (2007) .....	14

Mary Ellen Callahan, U.S. Dep't of Homeland Sec., <i>Privacy Issues in Border Searches of Electronic Devices</i> (2009).....	5
Microsoft, <i>Surface Pro 4</i> .....	14
Orin S. Kerr, <i>Searches and Seizures in a Digital World</i> , 119 Harv. L. Rev. 531 (2005).....	14, 27
Pew Research Ctr., <i>Mobile Fact Sheet</i> (Jan. 12, 2017) .....	8
Port Auth. of N.Y. & N.J., <i>Dec. 2017 Traffic Report: JFK</i> (Feb. 16, 2018).....	5
Port Auth. of N.Y. & N.J., <i>Dec. 2017 Traffic Report: LGA</i> (Feb. 16, 2018).....	5
Tanya Mohn, <i>Travel Boom: Young Tourists Spent \$217 Billion Last Year, More Growth Than Any Other Group</i> , Forbes (Oct. 7, 2013) .....	8
U.S. Customs and Border Protection, <i>Border Search of Electronic Devices</i> , Directive No. 3340-049A (Jan. 4, 2018).....	6, 7
U.S. Customs and Border Protection, <i>CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics</i> (Jan. 5, 2018).....	5, 6
U.S. Immigration and Customs Enf't, <i>Border Searches of Electronic Devices</i> , Directive No. 7-6.1 § 6.1 (Aug. 18, 2009).....	6, 7

## INTEREST OF *AMICI CURIAE*<sup>1</sup>

The American Civil Liberties Union (“ACLU”) is a nationwide, non-profit, non-partisan organization of more than 1 million members dedicated to defending the civil liberties and civil rights guaranteed by the Constitution. The New York Civil Liberties Union (“NYCLU”) is the New York 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, NYCLU, and EFF (collectively, “amici”) have been at the forefront of numerous state and federal cases addressing the right of privacy as guaranteed by the Fourth Amendment, and 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.

---

<sup>1</sup> 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.

## SUMMARY OF ARGUMENT

This case presents an important question about the extent of Fourth Amendment privacy rights in the digital age. Like Defendant-Appellant Thomas Perkins, 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 digital 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 without a warrant or individualized suspicion are likewise not justified by the rationales permitting routine border searches.

The facts of this case bear out these concerns. Acting on a tip from domestic investigators, and without seeking a warrant, U.S. Customs and Border Protection ("CBP") agents conducted a thorough search of the iPad that Mr. Perkins was

carrying in his luggage when he arrived at JFK International Airport after a flight from Canada. The search included viewing photos and searching for videos, (Hrg. 10:25–11:3; 58:5; 64:18–65:8), “look[ing] at . . . each individual app on the home screen” and subsequent screens (Hrg. 58:5-8), and opening two of those apps, (Hrg. 58:9-12)—conduct closely resembling the searches for which the Supreme Court required a warrant in *Riley*. 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 tens of millions who enter and exit the country through airports within the Second Department—carrying laptops, smartphones, and other portable 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. This information can be stored on the device itself or contained in cloud-based accounts that are accessible from the device. 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; *cf. People v. Weaver*, 12 N.Y. 3d 433, 447 (2009) (noting the need for “judicial oversight” to prevent the “unacceptable risk of abuse” created by “[t]echnological advances” in law enforcement tools). For these reasons, this Court should hold that federal agents violated the Fourth Amendment by searching Mr. Perkins’ 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.<sup>2</sup> This includes the more than 34 million international passengers who entered and exited the country through JFK and LaGuardia airports last year.<sup>3</sup> Of those, hundreds of thousands of travelers undergo secondary screenings, and 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,”<sup>4</sup> but border searches of electronic devices have more than tripled in two years. According to

---

<sup>2</sup> 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> (stating that more than 397 million international travelers were processed in fiscal year 2017).

<sup>3</sup> Port Auth. of N.Y. & N.J., *Dec. 2017 Traffic Report: JFK* (Feb. 16, 2018), [https://www.panynj.gov/airports/pdf-traffic/JFK\\_DEC\\_2017.pdf](https://www.panynj.gov/airports/pdf-traffic/JFK_DEC_2017.pdf); Port Auth. of N.Y. & N.J., *Dec. 2017 Traffic Report: LGA* (Feb. 16, 2018), [https://www.panynj.gov/airports/pdf-traffic/LGA\\_DEC\\_2017.pdf](https://www.panynj.gov/airports/pdf-traffic/LGA_DEC_2017.pdf).

<sup>4</sup> 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](https://www.dhs.gov/sites/default/files/publications/privacy_privacy_issues_border_searches_electronic_devices.pdf).

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.<sup>5</sup>

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") both have formal policies permitting border officials to read and analyze 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"].

---

<sup>5</sup> See *CBP FY17 Statistics*, *supra*; U.S. Customs and Border Protection, *CBP Releases Statistics on Border Device Searches* (Apr. 11, 2017), <https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0>.

ICE's policy, issued in 2009 and currently in force, authorizes ICE agents to search electronic devices "with or without individualized suspicion," and states that "a claim of privilege or personal information does not prevent the search of a traveler's information at the border." ICE Policy §§ 6.1, 8.6(1). 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 of an electronic device," 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. CBP policy thus permits searches without any individualized suspicion (1) when officers probe a device manually, irrespective of the invasiveness or duration of the search, or (2) when an "advanced search" is done to investigate a "national security concern." *Id.* § 5.1.4. Lastly, while CBP policy does not permit border officers from accessing cloud content, *id.* at § 5.1.2, such a limitation does not apply to searches by ICE, even when ICE only possesses a device because of a transfer from CBP, *id.* at § 2.7.

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 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<sup>6</sup>—who travel internationally at increasingly high rates.<sup>7</sup> 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.<sup>8</sup> 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.<sup>9</sup> 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.<sup>10</sup>

---

<sup>6</sup> Pew Mobile Fact Sheet.

<sup>7</sup> 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/>.

<sup>8</sup> *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/>.

<sup>9</sup> Pew Mobile Fact Sheet.

<sup>10</sup> Deloitte, *Digital Democracy Survey 5* (9th ed. 2015), <https://perma.cc/MX5G-2MKG>.

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% admitting that they even use their phones in the shower.” *Riley*, 134 S. Ct. at 2490. 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). Moreover, a person who travels with one electronic device often will travel with several, thus multiplying the digital data in their possession—and the privacy invasions of unfettered government searches. *See, e.g., United States v. Hassanshahi*, 75 F. Supp. 3d 101, 107 (D.D.C. 2014) (discussing seizure of traveler’s “laptop computer, multimedia cards, thumb drives, a camcorder, SIM cards, and a cell phone”).

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.

## **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 personal 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. Therefore, 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. *Id.* 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. Under the Fourth Amendment, a Warrant is Required to Search the Contents of an Electronic Devices 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.* at 2484–85. 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 is 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.<sup>11</sup>

Two recent opinions bolster the conclusion that *Riley* supports the need for greater protections here. In *United States v. Kolsuz*, No. 16-4687, 2018 WL 2122085 (4th Cir. May 9, 2018), the Fourth Circuit held that, following *Riley*, individualized suspicion is required for a forensic search of an electronic device seized at the border.<sup>12</sup> The panel majority explained that “even before the Supreme Court issued its 2014 decision in *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 smartphones and other digital devices” and the “uniquely sensitive nature of that information.” *Id.* at \*7-8. 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 \*8. 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

---

<sup>11</sup> 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).

<sup>12</sup> 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.” *Id.* at \*5.

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 \*9; *see also United States v. Vergara*, 884 F.3d 1309, 1313 (11th Cir. 2018) (J. Pryor, J., dissenting) (stating position that, pursuant to the analysis laid out in *Riley*, “a forensic search of a cell phone at the border requires a warrant supported by probable cause”).<sup>13</sup>

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 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.* (quoting *Riley*, 134 S. Ct. 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.

---

<sup>13</sup> As in *Kolsuz*, the defendant in *Vergara* did not challenge the manual search of his phone, *see* 884 F.3d at 1312.

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. When a traveler’s electronic device is searched at the border, the intrusion can be severe because a computer “is akin to a vast warehouse of information.” Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005). 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.” *Id.* Today’s devices are even more capacious. Laptops for sale in 2018 can store up to two terabytes,<sup>14</sup> the equivalent of more than 1.3 billion pages of text.<sup>15</sup> Even tablet computers—like Defendant-Appellant’s iPad here—can be purchased with up to a terabyte of storage.<sup>16</sup>

Smartphones also provide large storage capacities and can hold the equivalent of “millions of pages of text, thousands of pictures, or hundreds of

---

<sup>14</sup> See Apple, *Compare Mac models*, <https://www.apple.com/mac/compare/> (last visited Apr. 27, 2018).

<sup>15</sup> See LexisNexis, *How Many Pages in a Gigabyte?* (2007), [http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI\\_FS\\_PagesInAGigabyte.pdf](http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf).

<sup>16</sup> See Microsoft, *Surface Pro 4*, <https://www.microsoft.com/en-us/surface/devices/surface-pro-4/overview> (last visited Apr. 27, 2018); Apple, *Compare iPad Models*, <https://www.apple.com/ipad/compare/#ipad-pro-10-5,ipad> (last visited May 10, 2018) (iPads available with up to one half terabyte (512 GB) of storage).

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.<sup>17</sup>

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, 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,<sup>18</sup> medical records,<sup>19</sup> historical cell phone location data,<sup>20</sup> email,<sup>21</sup> privileged communications,<sup>22</sup> and associational information.<sup>23</sup>

---

<sup>17</sup> See, e.g., Google, *Pricing Guide*, <https://www.google.com/drive/pricing/> (last visited Apr. 27, 2018) (offering up to 10 terabytes of paid cloud storage).

<sup>18</sup> 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.”).

<sup>19</sup> See *Ferguson v. Charleston*, 532 U.S. 67, 78 (2001) (expectation of privacy in diagnostic test results).

<sup>20</sup> 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.”).

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 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.

---

<sup>21</sup> 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.”).

<sup>22</sup> 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).

<sup>23</sup> *Riley*, 134 S. Ct. at 2490 (“Mobile application software on a cell phone, or ‘apps,’ offer a range of tools for managing detailed information about all aspects of a person’s life. There are apps for Democratic Party news and Republican Party news . . . .”); *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 . . . .”).

A regime of suspicionless device searches also implicates First Amendment freedoms, including the right to freedom of speech (which itself includes the rights to communicate and receive or access information, and the right to speak anonymously), freedom of the press (including the right to gather news and protect confidential sources), and freedom of private association. 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 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.

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*, 2018 WL 2122085, at \*6 (“[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. That is, warrantless border searches of electronic devices do not sufficiently advance these goals. *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).

As with the search-incident-to-arrest exception, where warrantless and suspicionless searches are 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*, 2018 WL 2122085, at \*6. 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,” *id.*, 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 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 neither need to 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”).<sup>24</sup> 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 the

---

<sup>24</sup> Unlike CBP’s 2018 policy, ICE’s 2009 policy does not prohibit border searches of cloud content.

destruction of evidence and that, in any event, any such possibilities do “not justify dispensing with the warrant requirement across the board”).

Of course, where border officers have actual probable cause to believe contraband data is stored on a device, they can secure a search warrant—as they did for the later, post-arrest forensic search of Mr. Perkins’ device in this case. (*See* Trial Tr. 350, 354, 358–59 (description of forensic search); Ex. A to Supp. Mot. to Suppress (filed Nov. 3, 2015) (warrant for forensic search)). And in rare instances where there is truly no time to go to a judge, the exigent circumstances exception may apply. *See Riley*, 134 S. Ct. at 2486.

Even assuming that conducting 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*, 2018 WL 2122085, at \*8. As a 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*, 2018 WL

2122085, at \*7 (“[E]ven before the Supreme Court issued its 2014 decision in *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 individual 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. Of course, 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, device searches at the border 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. Perkins’ experience demonstrates, officers can and do use threats of confiscation to extract device passcodes from travelers, search the devices’ content for lengthy periods outside the travelers’ presence, and retain the contents of the devices. *See Post-Hr’g Mem. of Law in Supp. of Pretrial Mot. to Suppress* at 6–7.

Requiring a warrant for border device searches is both feasible and necessary to satisfy the requirement of reasonableness under the Fourth Amendment. *See Riley*, 134 S. Ct. at 2493 (“Recent technological advances . . .

have . . . made the process of obtaining a warrant itself more efficient.”). The Supreme Court has contemplated this warrant process at the border. *See Ramsey*, 431 U.S. at 623–24; *Montoya de Hernandez*, 473 U.S. at 547 & n.13.<sup>25</sup>

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

In this case, Mr. Perkins was subject to a manual search of his phone absent a warrant.<sup>26</sup> Although most cases requiring individualized suspicion for searches of electronic devices at the border have addressed forensic searches, *see, e.g., Kolsuz* 2018 WL 2122085, at \*5; *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

---

<sup>25</sup> 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). The remainder 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. Molina-Isidoro*, 267 F. Supp. 3d 900 (W.D. Tex. 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).

<sup>26</sup> Following Mr. Perkins’ arrest and detention, investigators conducted a forensic search pursuant to a warrant. (*See* Trial Tr. 350, 354, 358–59 (description of forensic search); Ex. A to Supp. Mot. to Suppress (filed Nov. 3, 2015) (warrant for forensic search)).

level of intrusiveness a manual device search can entail.” *Alasaad*, 2018 WL 2170323, at \*20.

In the case of manual searches, like the one at issue in this case, 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.<sup>27</sup> 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.<sup>28</sup> “Manual” searches can access emails, voicemails, text messages, call logs, contact lists, photographs, videos, calendar entries, 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

---

<sup>27</sup> In July 2017, CBP publicly announced that its agents are not supposed to access cloud-stored data during border searches of electronic devices. The search at issue in this case took place on April 18, 2014, 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>.

<sup>28</sup> 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 Apr. 27, 2018).

the traveler's navigation history.<sup>29</sup> 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 even more 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 search unsuccessfully attempted by border agents using a Cellebrite machine in this case, are likewise highly invasive. Forensic searches typically begin with an agent making a mirror-image copy of a device's entire hard drive or other digital storage repository, including all active files, deleted files,<sup>30</sup> allocated and unallocated file space,<sup>31</sup> and metadata. That copy is then analyzed using powerful programs that read and sort every file and byte stored on the device, including deleted files and other files that the device user may not even be aware exist.

---

<sup>29</sup> See Google, *Google Maps Help*, <https://support.google.com/maps/answer/6258979?co=GENIE.Platform%3DDesktop&hl=en> (last visited Apr. 27, 2018).

<sup>30</sup> "[M]arking a file as 'deleted' normally does not actually delete the file; operating systems do not 'zero out' the zeros and ones associated with that file when it is marked for deletion." Kerr, 119 Harv. L. Rev. at 542.

<sup>31</sup> "'Unallocated space is space on a hard drive that contains deleted data . . . that cannot be seen or accessed by the user without the use of forensic software.'" *Cotterman*, 709 F.3d at 958 n.5 (citation omitted).

The forensic search tools used by the government can extract and analyze tremendous quantities of data. In one 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, 40–41 & n.3 (D.D.C. 2015). Any time a device seized at the border remains in government custody, it is potentially subject to a forensic search. And indeed, Mr. Perkins’ device was forensically searched after his initial detention and arrest, but only after agents had gotten a warrant.<sup>32</sup> (Hrg. 60:3-4; Trial Tr. 350; Ex. A to Supp. Mot. to Suppress).

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. 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

---

<sup>32</sup> Although CBP and ICE policies do not require a warrant for such forensic searches, the fact that agents got a warrant before performing a forensic search of Mr. Perkins’ device demonstrates that doing so is not impracticable.

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. Perkins’ electronic devices without a warrant based on probable cause.

Respectfully submitted,



NATHAN FREED WESSLER

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

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

Christopher Dunn  
Aadhithi Padmanabhan  
NEW YORK CIVIL  
LIBERTIES UNION  
FOUNDATION  
125 Broad Street,  
19<sup>th</sup> Floor  
(212) 607-3300 (phone)  
cdunn@nyclu.org  
apadmanabhan@nyclu.org

Dated: May 15, 2018  
New York, N.Y.