UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

GHASSAN ALASAAD, NADIA ALASAAD, SUHAIB ALLABABIDI, SIDD BIKKANNAVAR, JÉRÉMIE DUPIN, AARON GACH, ISMAIL ABDEL-RASOUL a.k.a. ISMA'IL KUSHKUSH, DIANE MAYE, ZAINAB MERCHANT, MOHAMMED AKRAM SHIBLY, and MATTHEW WRIGHT, Plaintiffs, v. KIRSTJEN NIELSEN, Secretary of the U.S. Department of Homeland Security, in her official capacity; KEVIN McALEENAN, Acting Commissioner of U.S. Customs and Border Protection, in his official capacity; and THOMAS HOMAN, Acting Director of U.S. Immigration and Customs Enforcement, in his official capacity, Defendants.	Civil Action No. 17-cv-11730-DJC Hon. Denise J. Casper

BRIEF OF AMICI CURIAE THE BRENNAN CENTER FOR JUSTICE, CENTER FOR DEMOCRACY & TECHNOLOGY, THE R STREET INSTITUTE, AND TECHFREEDOM

Matthew S. Shapanka (BBO #690394)
Covington & Burling LLP
One CityCenter
850 Tenth Street NW
Washington, D.C. 20001
(202) 662-5136
mshapanka@cov.com

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

DIRECTIVES

OTHER AUTHORITIES

INTERESTS OF THE AMICI

The Brennan Center for Justice at NYU School of Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice. The Center's Liberty and National Security (LNS) Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. The LNS Program is particularly concerned with domestic surveillance and related law enforcement policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on First and Fourth Amendment freedoms.[1]

The Center for Democracy & Technology (CDT) is a non-profit, public interest organization focused on privacy and civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes constitutional and democratic values of free expression, privacy, and individual liberty in the digital age.

The R Street Institute (R Street) is a non-profit, non-partisan public-policy research organization. R Street's mission is to engage in policy research and educational outreach that promotes free markets, as well as limited yet effective government, including properly calibrated legal and regulatory frameworks that support national security while safeguarding privacy and individual liberty.

TechFreedom is a non-profit, non-partisan think tank dedicated to educating policymakers, the media, and the public about technology policy. TechFreedom defends the

[1] This brief does not purport to represent the position of NYU School of Law.

freedoms that make technological progress both possible and beneficial, including the privacy rights protected by the Fourth Amendment, the crown jewel of American civil liberties.

INTRODUCTION

Amici file this brief in support of plaintiffs' claim that warrantless, suspicionless border searches of digital devices, such as laptop computers and cellular telephones, violate the First and Fourth Amendments to the Constitution because such devices contain great quantities of extremely sensitive information.

In its newly revised Directive governing searches of electronic devices, U.S. Customs and Border Protection ("CBP") justifies suspicionless searches by citing to case law supporting the notion of a "border exception" to the Fourth Amendment's warrant requirement.[2] In one of these cases, from 2004, the Supreme Court sustained the government's search of a traveler's gas tank without reasonable suspicion. *United States v. Flores-Montano*, 541 U.S. 149 (2004). In another, from 1977, the Court upheld the warrantless search of the contents of eight envelopes from Thailand. *United States v. Ramsey*, 431 U.S. 606 (1977). Other cases sanctioned warrantless searches of one shipping container, *United States v. Boumelhem*, 339 F.3d 414 (6th Cir. 2003), sixteen cardboard boxes, *United States v. Odutayo*, 406 F.3d 386 (5th Cir. 2005), and suitcases, *United States v. Ezeiruaku*, 936 F.2d 136 (3d Cir. 1991). As amici representing diverse viewpoints within the privacy and civil liberties community, we write to highlight the obvious, dramatic differences between searches of gas tanks, envelopes, boxes, and suitcases, and searches of electronic devices.

[2] U.S. Customs and Border Protection, Border Search of Electronic Devices, CBP Directive No. 3340-049A at ¶ 4 (Jan. 4, 2018).

The case before this Court is a classic case of government overreach. The government seeks to take advantage of decades-old precedents that address physical belongings by applying them to digital devices. However, digital is different. The digital content subject to suspicionless searches paints a detailed picture of a traveler's entire life—from texts, call logs, mechanical voicemails, emails, and social media messages to photos, documents, dating apps, address books, calendars, browsing history, purchases, recent locations, bank statements, money transfers sent using Venmo or PayPal, music playlists, books, news articles, diagnostic, weight loss, fertility tracking, and other health apps, and perhaps even the home security app that can stream, record, and store videos from a webcam inside the traveler's living room.[3]

The need to address this overreach is pressing because digital content is becoming ever more prevalent. If most estimates are correct, by 2020 approximately 80 percent of international travelers will carry a smart phone.[4] Roughly half of American passengers may also carry their tablet or computer (or keep it at home, but sync its contents with their smart phone).[5] With the pervasiveness of digital devices steadily (and rapidly) climbing, CBP officials have dramatically

[3] *See* The SimpliSafe SimpliCam, https://simplisafe.com/simplicam-security-camera (last visited Jan. 24, 2018).

[4] *See* The Economist, *Planet of the Phones* (Feb. 26, 2015) (based on estimates that 80% of the world's adults will own a smart phone in 2020), https://www.economist.com/news/leaders/21645180-smartphone-ubiquitous-addictive-and-transformative-planet-phones.

[5] *See* Pew Research Ctr., *Mobile Fact Sheet* (Jan. 12, 2017), *available at* http://www.pewinternet.org/fact-sheet/mobile/.

increased their searches of these treasure troves of data—by more than 60 percent within the past year alone.[6]

The Supreme Court recently recognized that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house." *See Riley v. California*, 134 S. Ct. 2473, 2491 (2014) (emphasis in the original).[7] In this case, the Court must likewise acknowledge that the sheer quantity and quality of data contained on a person's digital device makes that device far different from the physical items traditionally searched at the border, and the CBP Directive's new limitations on electronic searches are a far cry from the individualized suspicion that the Fourth Amendment's "reasonableness" standard requires. Moreover, such new rules only apply to CBP, leaving policy on suspicionless searches by U.S. Immigration and Customs Enforcement ("ICE") unchanged.[8] For these reasons, we urge the Court to declare that the Defendants' policies and practices violate the First and Fourth Amendments.

ARGUMENT

I. Border Searches of Digital Devices Must Require Individualized Suspicion.

A. Digital Devices Contain Vast Quantities of Information That Far Exceed What Travelers Have Traditionally Carried When Crossing the Border.

The purported "exception" to the Fourth Amendment's warrant requirement at the border was developed in the context of searches limited by "physical realities"—namely, that travelers

[6] Press Release, *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics*, CBP (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and.

[7] In *Riley*, the unique quantity and quality of information contained on digital devices led the Court to reject the extension of a different "exception" to the Fourth Amendment to such devices.

[8] *See* Immigration and Customs Enforcement, Border Searches of Electronic Devices, ICE Directive No. 7-6.1 (Aug. 18, 2009).

can only carry so many pieces of luggage, only pack so many items inside that luggage, and only check so many boxes onto a flight. *Cf. Riley*, 134 S. Ct. at 2489 ("Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy."). In the digital world, such limitations are practically nonexistent, and they become increasingly negligible as the amount of data travelers carry continues to skyrocket.

When *Riley* was decided in 2014, for example, the best-selling smart phone came with a minimum storage capacity of 16 gigabytes (GB)—the equivalent of millions of physical pages of text, or roughly the same amount of storage space as a typical home desktop computer in 2004.[9] Today, less than four years later, the minimum storage capacity of that smart phone has quadrupled to 64 GB, and can reach a staggering 256 GB.[10] Crossing the border with 256 GB in your pocket is the physical equivalent of traveling with approximately 128 million pages of text (for reference, the entire seven-part *Harry Potter* series contains only 4,224 pages).[11,12] Traveling with an iPad Pro tablet (with a maximum 512 GB of data) is the equivalent of carrying

[9] *See* Brief for Center for Democracy & Technology and Electronic Frontier Foundation as Amici Curiae in *Riley v. State of California*, at 6 (Aug. 2013), *available at* https://cdt.org/files/pdfs/Riley-v-California-Amicus-Brief.pdf.

[10] *See* The Apple iPhone X, https://www.apple.com/iphone-x/specs/ (last visited Jan. 24, 2018).

[11] *See, e.g.*, Orin S. Kerr, *Searches and Seizures in a Digital World*, 199 Harv. L. Rev. 531, 542 (2005) (explaining that an 80 GB hard drive is equivalent to 40 million physical pages, or one floor of an academic library).

[12] Mekado Murphy, *Potter's Magic Numbers*, N.Y. Times (Jul. 14, 2009), https://artsbeat.blogs.nytimes.com/2009/07/14/potters-magic-numbers/.

the contents of approximately six floors of an academic library—the same number of floors as the Harvard Law Library.[13]

In addition, the vast storage capacity of digital devices makes it increasingly impractical, if not impossible, to "pack" your digital devices with only the trip-specific items you need, as you would pack your physical suitcase. *See United States v. Cotterman*, 709 F.3d 954, 965 (9th Cir. 2013) ("When packing traditional luggage, one is accustomed to deciding what papers to take and what to leave behind."). Moreover, even if a traveler believes she "emptied" her digital device of all the data that she does not need for her trip, data generally remains on the device in some form, even after it has been "deleted." In one study, a security software team purchased twenty different phones on eBay that had been restored to their factory settings and was still able to recover 40,000 photos, 750 emails, 250 contacts with names and addresses, and even sensitive documents (such as a loan application and a completed sexual harassment course).[14] As a result, searching a digital device is starkly different from searching a person's travel bag—a more apt comparison is searching "not only what [a] bag contained on the current trip, but everything it [has] ever carried." *Id*.

Compounding the problem is the proliferation of cloud-based storage solutions, which cache onto smart phones vast quantities of data to enable consumers to access and interact with their data on the go, even when disconnected from the Internet. Google Drive, for example,

---

[13] *See* Orin S. Kerr, *supra* n. 11, at 542; *see also* The Apple iPad Pro, https://www.apple.com/ipad-pro/specs/ (last visited Jan. 24, 2018); Harvard Law School: Library Maps, http://hls.harvard.edu/library/about-the-library/library-maps/ (last visited Jan. 24, 2018).

[14] Pete Pachal, *Hard Proof That Wiping Your Phone Doesn't Actually Delete Everything*, Mashable (Jul. 9, 2014), http://mashable.com/2014/07/09/data-wipe-recovery-smartphones/#NMovhG8YESqz.

automatically syncs spreadsheets, word processing documents, and PowerPoint presentations with Google Docs, which can be viewed offline.[15] Similarly, Microsoft Outlook allows users to access certain mailbox features offline,[16] Facebook offers an "offline" mode in an effort to reach users with poor service connections,[17] and Amazon Prime users can now download movies, episodes, and other content from Amazon's video streaming service.[18] As a result, it is often difficult to distinguish where a device's hardware ends and where the "cloud" begins.[19]

B. Digital Devices Store Extremely Sensitive, Personal Information—Making Them Pocket-Sized Doors Into Their User's Entire Life.

Not only is there a vast *quantity* of information subject to suspicionless searches of digital devices at the border, but the *quality* of that information is increasingly revealing. As digital devices and the apps that they host have grown more advanced, they have become a progressively constant presence in their users' lives—resulting in their contents conveying an astoundingly accurate, intimate picture of their users' daily routines. *Riley*, 134 S. Ct. at 2484 ("[M]odern cell phones . . . are now such a pervasive and insistent part of daily life that the

---

[15] Melanie Pinola, *Make Google docs, spreadsheets, and presentations work offline*, ITWorld (Apr. 26, 2013), https://www.itworld.com/article/2709713/consumerization/make-google-docs--spreadsheets--and-presentations-work-offline.html.

[16] Microsoft Support: Using Outlook Web App offline, https://support.office.com/en-us/article/Using-Outlook-Web-App-offline-3214839C-0604-4162-8A97-6856B4C27B36 (last visited Jan. 24, 2018).

[17] Sarah Perez, *Facebook Gets An Offline Mode*, TechCrunch (Dec. 10, 2015), https://techcrunch.com/2015/12/10/facebook-gets-an-offline-mode/.

[18] Amazon Help & Customer Service, *Download Prime Video Titles*, https://www.amazon.com/gp/help/customer/display.html?nodeId=201460820 (last visited Jan. 24, 2018).

[19] Note that although CBP's new policy prohibits searches of remote data that is not "resident" on a device, CBP Directive 3340-049A ¶ 5.1.2, ICE's policy contains no such restriction. *See* ICE Directive No. 7-6.1, ¶ 6.1 (authorizing searches of electronic devices "with or without suspicion," with no distinction between "basic" searches and "advanced" (forensic) searches).

proverbial visitor from Mars might conclude they were an important feature of human anatomy."). Moreover, this "picture" of daily life may span several years, due to devices' vast storage capacities highlighted above. *Id.* at 2489 ("The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet.").

On average, American users look at their smart phones 47 times per day.[20] Eighty-nine percent of users check their messages, read the news, or interact with other smart phone services within one hour of waking up.[21] Nearly three-quarters of users report being within five feet of their phones most of the time. *Id.* at 2490, *citing* Harris Interactive, *2013 Mobile Consumer Habits Study* (Jun. 2013). When traveling, people use digital devices even more frequently for navigation, recommendations, financial management, health information, photos, videos, and unimpeded communications with family and friends—making them "digital umbilical cords to what travelers leave behind at home or at work." *See United States v. Saboonchi*, 990 F. Supp. 2d 536, 557–58 (D. Md. 2014).

Many smart phones and tablets combine functions that few contemplated would ever be performed by one single device—and these functions reveal information increasingly sensitive and private in nature. They contain information that travelers would likely hesitate to carry with them in the first place—such as "apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; [and] apps for improving your romantic life."

---

[20] *See* Deloitte, *2017 Global Mobile Consumer Survey: U.S. edition* (2017), https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/global-mobile-consumer-survey-us-edition.html.

[21] *Id*.

Riley 134 St. Ct. at 2490. These apps can reveal infirmities and medical conditions, financial information, and romantic interests. Apps may also reveal a user's political associations and activities—for example, one left-leaning app enables third-party voters in swing states to identify and swap votes with Democratic supporters in safe states.[22] A right-leaning app provides ratings of companies based on their stances on various social issues such as abortion and the Second Amendment.[23] Other apps may betray the fact that a traveler is a staunch opponent of the Trump Administration.[24]

In addition, the versatility of digital devices has made them critical to most people's professional lives. As a result, private communications, documents, and other materials typically afforded the apex of legal protections in any other context may face being searched and seized without a warrant at the border. Lawyers, for example, are highly likely to have tomes of privileged client communications and attorney work product on their devices.[25] Corporate executives may carry proprietary data and sensitive trade secrets that can move markets. Doctors may have confidential information about their patients and their maladies. Scientists and

[22] *See, e.g.*, Zachary Crockett, *Third-party voters are "trading votes" with Clinton voters to defeat Trump*, Vox (Nov. 3, 2016), https://www.vox.com/policy-and-politics/2016/11/3/13478042/third-party-clinton-vote-trading.

[23] Jeff Green, *This Website Scores Companies on Their Conservative Values*, Bloomberg.com (Oct. 17, 2017), https://www.bloomberg.com/news/articles/2017-10-17/website-2ndvote-scores-companies-on-their-conservative-values.

[24] Heather Dockray, *7 extremely useful sites and apps to help you organize in Trump's America*, Mashable (Nov. 29, 2016), http://mashable.com/2016/11/29/trump-organizing-apps-sites/#VWEiK1XFEqqi.

[25] Bruce Green, *The Risk of Border Searches for Lawyers*, Big Law Business (Aug. 22, 2017), https://biglawbusiness.com/the-risk-of-border-searches-for-lawyers-perspective/.

inventors may possess patentable or classified technology schematics.[26] Journalists may carry drafts of work product and the names and contact information of confidential sources.[27]

Importantly, the sensitivity of the data typically contained on a person's device is at least as invasive as strip searches and body cavity searches, if not more so.[28] Indeed, cell phones today often contain highly intimate images of spouses or romantic partners.[29] Americans have a very reasonable expectation that such sensitive information cannot be searched on a whim—or even incident to their arrest—leading to unusually uncomfortable and unexpected invasions of their privacy and dignity at the border.

II. Customs and Border Protection's New Directive Fails to Address the Vastness and Sensitivity of Digital Data.

A. The Directive Still Authorizes Suspicionless Searches of Every Device—of Every Person—Crossing the Border.

A typical digital device contains an enormous amount of detailed, sensitive data—data that is readily available at the fingertips of anyone with access to the device. As a result, CBP's new disparate treatment of "advanced" (forensic) searches versus "basic" searches does not

---

[26] *See, e.g.*, Kaveh Waddell, *A NASA Engineer Was Required to Unlock His Phone at the Border*, The Atlantic (Feb. 13, 2017), https://www.theatlantic.com/technology/archive/2017/02/a-nasa-engineer-is-required-to-unlock-his-phone-at-the-border/516489/; Brian Owens, *Cybersecurity for the travelling scientist*, Nature (Aug. 2, 2017), https://www.nature.com/news/cybersecurity-for-the-travelling-scientist-1.22379.

[27] Andrea Peterson, *U.S. border agents stopped journalist from entry and took his phones*, Wash. Post (Nov. 30, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/11/30/u-s-border-agents-stopped-journalist-from-entry-and-took-his-phones/?utm_term=.9d985e075f85.

[28] Matthew B. Kugler, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. Chi. L. Rev. 1165, 1166–67 (2014).

[29] *See, e.g.*, Charlie Savage & Ron Nixon, *Privacy Complaints Mount Over Phone Searches at U.S. Border Since 2011*, N.Y. Times (Dec. 22, 2017), https://www.nytimes.com/2017/12/22/us/politics/us-border-privacy-phone-searches.html ("I told them my religion prohibits that other men see my wife without the hijab (the head cover) and in some pics she was partially nude").

resolve the constitutional issues surrounding both types of searches. It also changes nothing about the ICE policy, which authorizes suspicionless searches regardless of agents' means or methods. ICE Directive No. 7-6.1, ¶ 6.1.

Under the CBP Directive, a "basic" search can involve scrolling through a traveler's entire device and everything "resident" on it—be it stored locally, cached, or transmitted before the device was disconnected from the Internet. CBP Directive 3340-049A, ¶ 5.1.2. Considering what anyone can find on a device when given free license to browse through it, it is clear that such searches are anything but "basic," even without the support of special forensic "tools." Moreover, the Directive empowers CBP officials to require travelers to "present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents," *id*. at 3340-049A, ¶ 5.3.1, meaning that travelers can be compelled to unlock and decrypt their devices and all the information contained in them—including sensitive documents such as bank statements, encrypted messages, or even password-protected apps that allow users to list all of their *other* passwords in one convenient, accessible place.[30]

B. Even When the Directive Requires Suspicion, the "National Security" Exception Renders This Protection Toothless.

In some circumstances, the new Directive requires "reasonable suspicion"—but with an exception for national security concerns that nullifies any heightened degree of protection this requirement was meant to provide. The exception swallows the rule, even assuming that "reasonable suspicion" (and not probable cause) is the correct Fourth Amendment standard. For example, the "advanced" (forensic) search's reasonable suspicion requirement can be circumvented once an officer believes that a "national security concern" is present. Factors for

[30] *See, e.g.*, Dashlane, https://www.dashlane.com/ (last visited Jan. 25, 2018).

identifying such national security-related concerns are remarkably vague, such as "a relevant national security-related lookout in combination with *other articulable factors as appropriate*." CBP Directive 3340-049A, ¶ 5.1.4 (emphasis added).

Moreover, CBP's purported authority to conduct such sweeping, suspicionless searches is derived from what is often cited as a "national security concern"—protecting the border. As a result, CBP officials can easily reverse engineer a "national security concern" to justify the majority, if not all, of even the most advanced searches of digital devices, with little to no individualized suspicion.

C. The Directive's Protections for Privileged Data Are Inadequate.

The Directive's requirement that traveling attorneys identify the "specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars" of privileged information resident on their devices in order to protect such information during a border search, *id*. at 3340-049A, ¶ 5.2.1.1, is simply impractical given the interspersed nature of data contained on a device, as well as the logistics of international travel. Even if done with care, the process would take hours of time that the attorney traveler does not have at the airport, could still miss some privileged information, and would inevitably leave some data intact because, as discussed above, deleted data is oftentimes recoverable through forensic tactics.[31] In addition, the rest of CBP's review process for privileged information—which involves contacting the CBP Associate/Assistant Chief Counsel office and engaging a "Filter Team"—likely will take several *more* hours' worth of time. Moreover, the heightened protections applied to attorney privileged information do not apply to other types of sensitive professional data. Journalists and business executives, for example, are only protected by

[31] *See* Pachal, *supra* note 14.

"applicable federal law" (which may be significantly lessened in the border context) as well as undefined "CBP policies." *Id*. at 3340-049A, ¶¶ 5.2.2–5.2.3.

CONCLUSION

The information contained on a traveler's digital device is far more voluminous and sensitive than most could have imagined just a few short years ago—let alone decades ago, when the courts initially formulated the so-called "border exception" search doctrine. More often than not, a traveler's device will contain the intricate, intimate details of their personal and professional lives, and compelling their disclosure without any suspicion "places the liberty of every man at the hands of every petty officer."[32] For these reasons, the Court should declare that Defendants' practices violate the First and Fourth Amendments.

Dated: February 2, 2018

By: /s/ *Matthew S. Shapanka*
Matthew S. Shapanka (BBO #690394)
Covington & Burling LLP
One CityCenter
850 Tenth Street NW
Washington, D.C. 20001
(202) 662-5136
mshapanka@cov.com

Counsel for Amici Curiae

[32] John Adams, Legal Papers of John Adams, Vol. 2 141—42 (L. Kinvin Wroth & Hiller B. Zobel eds., Harvard University Press 1965).

CERTIFICATE OF SERVICE

I certify that on February 2, 2018, a copy of the foregoing was filed electronically via the Court's ECF system, which effects services upon counsel of record.

/s/ *Matthew S. Shapanka*
Matthew S. Shapanka