No. 20-10059

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

GEORGE ANIBOWEI,

Plaintiff-Appellant,

v.

CHAD F. WOLF,

Acting Secretary, U.S. Department of Homeland Security, et al.,

Defendants-Appellees.

On appeal from the United States District Court
for the Northern District of Texas, Dallas Division

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF APPELLANT SEEKING REVERSAL

ALAN BUTLER
Counsel of Record
MEGAN IORIO
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
butler@epic.org

Counsel for Amicus Curiae *EPIC*

June 9, 2020

SUPPLEMENTAL CERTIFICATE OF INTERESTED PARTIES

George Anibowei v. Chad Wolf, et al., No. 20-10059

Pursuant to Fed. R. App. P. 26.1 and 29(c), *Amicus Curiae* Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

The undersigned counsel of record certifies that the following listed persons and entities as described in the fourth sentence of Rule 28.2.1 have an interest in the outcome of this case. These representations are made in order that the judges of this court may evaluate possible disqualification or recusal.

The Electronic Privacy Information Center ("EPIC"), *amicus curiae*.

ALAN BUTLER
MEGAN IORIO
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
butler@epic.org

*/s/ Alan Butler*_____
Alan Butler
Counsel of Record

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF AMICUS

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy issues.[1]

EPIC routinely participates as *amicus curiae* in cases that involve constitutional protections and emerging technologies. *See, e.g.,* Brief for EPIC et al. as *Amici Curiae* Supporting Respondent, *Kansas v. Glover*, 140 S. Ct. 1183 (2020) (No. 18-556) (arguing that widespread use of automated license plate readers required reasonable suspicion for vehicular stops to be predicated on more than the suspended license of the registered owner); Brief for EPIC et al. as *Amici Curiae* Supporting Petitioner, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402) (arguing that technological changes since the era of analog phones justify departing from the third-party doctrine); Brief for EPIC et al. as *Amicus Curiae* Supporting Petitioner, *Packingham v. North Carolina*, 137 S. Ct 1730 (2017) (No. 15-1194) (arguing that the First Amendment protects the right to access speech from the privacy of a personal electronic device); Brief for EPIC et al. as *Amici Curiae* Supporting Petitioner, *Riley v. California*, 573 U.S. 373 (2014)

[1] The parties consent to the filing of this *amicus curiae* brief. In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

(No. 13-132) (arguing that, because modern cell phone technology provides access to an extraordinary amount of personal data, a warrantless search of a person's cell phone is a substantial and unnecessary infringement of privacy); Brief for EPIC as *Amicus Curiae* Supporting Appellant, *Jackson v. McCurry*, 762 Fed. Appx. 919 (11th Cir. 2019) (No. 18-10231) (urging the court to limit searches of students' phones to "circumstances when it is strictly necessary" in light of *Riley*); Brief for EPIC as *Amicus Curiae* Supporting Appellant, *United States v. Miller*, No. 18-5578 (6th Cir. filed Oct. 17, 2018) (arguing that, because the Government could not establish the reliability of Google's email screening technique, its use constituted an unreasonable search); Brief for EPIC as *Amicus Curiae* Supporting Petitioner, *State v. Andrews***,** 197 A.3d 200 (N.J. Sup. Ct. App. Div. 2018), *leave to appeal granted*, No. 82209 (N.J. May 3, 2019) (arguing that *Riley* and *Carpenter* prohibit the government from compelling decryption of a cell phone).

SUMMARY OF THE ARGUMENT

This Court must now decide whether the border search exception to the Fourth Amendment warrant requirement should be extended to searches of cell phones. The Supreme Court has twice declined—and not once agreed—to extend pre-digital era exceptions to the warrant requirement to searches of cell phones. The Court found in both *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and *Riley v. California*, 573 U.S. 373 (2014), that the balance of individual and government interests weighed in favor of the substantial privacy interests an individual has in their cell phone data. For the same reason, this Court should decline to extend the border search exception to searches of cell phones.

First, the Supreme Court has clearly established that individuals have a constitutionally protected privacy interest in the contents of their cell phones. As the Court in *Riley* recognized, cell phones are both quantitatively and qualitatively different than other containers because of the enormous amount of private data stored on and accessible from the devices. The privacy and confidentiality interests at stake in this case are even more acute because the Plaintiff is an attorney whose phones contain sensitive client information. Indeed, the American Bar Association has called on courts and legislatures to establish a warrant requirement for searches of cell phones at the border.

Second, as with the search incident to arrest exception at issue in *Riley*, the search of a cell phone at the border bears little resemblance to the searches that traditionally justified the border search exception. Historically, the border search exception protected the government's interests in preventing contraband from entering the country and regulating the admission of noncitizens to the United States. But cell phones cannot hold the types of contraband that have justified the border search exception, and digital contraband does not primarily enter the country through physical ports of entry. Extending the border search exception to evidence of border crimes would broaden the exception in a way that the Court in *Riley* found untenable. Finally, Plaintiff in this case is a citizen of the United States whose admission should be secure upon identification, leaving no immigration justification for a search. Officers at the border should have obtained a warrant prior to searching Mr. Anibowei's cell phones.

ARGUMENT

In *Riley v. California* and *Carpenter v. United States,* the Supreme Court declared that individuals have a constitutional right to privacy in their cell phone data. The Court assessed "on the one hand, the degree to which [the search of a cell phone] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests," and determined that the individual's privacy interests were more substantial. *Riley*, 573

U.S. at 385 (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). That was so even in the search incident to arrest context, where arrestees have a "significantly diminished" expectation of privacy. *Id*. at 386. Indeed, "the fact of 'diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely.'" *Carpenter,* 138 S. Ct. at 2219 (quoting *Riley*, 573 U.S. at 392).

Constitutional protections for cell phone data do not simply disappear at the border. After all, "the Fourth Amendment protects people, not places." *Katz v. United States*, 389 U.S. 347, 351 (1967). An individual's cell phone data is equally protected at home, during an arrest, and when they travel. Cell phones contain vast quantities of sensitive personal information, stored on and accessible from the device wherever it goes. The intrusion of a cell phone search is particularly acute for an individual, like the plaintiff in this case, whose phone contains confidential and privileged information about clients with interests adverse to the United States.

Furthermore, the government has a limited interest in and authority to conduct warrantless searches under the border search exception. Cell phone data "does not fit neatly under existing precedents," including the border search exception. *Carpenter,* 138 S. Ct. at 2214. While the pre-digital border search exception, like the search incident to arrest exception, might "strike the right balance in the context of physical objects, neither of its rationales has much force

with respect to digital content on cell phones." *Riley*, 573 U.S. at 386. At the border, the "privacy-related concerns are weighty enough" in the cell phone context to overcome the government's limited interest in conducting warrantless searches. *Id.* at 392. Indeed, permitting warrantless searches of cell phones at the border would leave travelers "at the mercy of advancing technology." *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)).

This Court should follow the reasoning of *Riley* and *Carpenter* and decline to extend the border search exception to cell phones.

I. An individual has a constitutionally protected privacy interest in the contents of their cell phone.

A. Cell phones provide access to a vast amount of personal information.

Modern cell phones have fundamentally changed the scope of searches at the border. Cell phones "place vast quantities of personal information literally in the hands of individuals," making a search of a cell phone "bear[] little resemblance" to the searches traditionally carried out at the border. *Riley*, 573 U.S. at 386. Cell phone data "implicates privacy concerns far beyond those considered" in pre-digital era cases concerning the border search exception. *Carpenter*, 138 S. Ct. at 2220.

As Chief Justice Roberts wrote in *Riley*, "[t]he term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also

happen to have the capacity to be used as a telephone." 573 U.S. at 393. From bank records to medical records to photos, videos, and internet browsing history, Americans' cell phones are a window into their personal lives. Today, "a digital record of nearly every aspect of [Americans'] lives" is accessible through one highly portable device. *Id.* at 375.

Smartphones are ubiquitous; 81% of Americans own one. Pew Res. Ctr., *Mobile Fact Sheet* (June 12, 2019).[2] Indeed, the devices "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of the human anatomy." *Riley,* 573 U.S. at 385. The ubiquity of cell phones—and the need in modern society to have them on one's person at all times—implicates heightened constitutional concerns because any rule allowing warrantless searches will inevitably "run[] against everyone." *Carpenter*, 138 S. Ct. at 2218.

Cell phones "differ in both a quantitative and a qualitative sense" from non-digital objects. *Riley*, 573 U.S. at 393. Indeed, "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity." *Id.* In 2014, when *Riley* was decided, the top-selling smartphone had "a standard capacity of 16 gigabytes . . .[, which] translates to millions of pages of text, thousands of pictures, or hundreds of videos." *Riley*, 573 U.S. at 394. Today, the

[2] https://www.pewinternet.org/fact-sheet/mobile/.

minimum storage available on Apple's current line of iPhones is 64GB. Apple, *Compare iPhone Models* (2020).[3] That is over 1 million word documents, 200,000 PDF documents, almost 40,000 photos, 42 full length movies, and almost 15,000 songs. iClick, *How Big is a Gig?* (2013).[4] Top-of-the-line iPhones—the iPhone 11 Pro and iPhone 11 Max—can now store 512GB of data. Apple, *Compare iPhone Models* (2020).[5] Samsung's Galaxy S10+ has a 1TB capacity, which is roughly 64 times as much storage as the largest smartphones available at the time *Riley* was decided.[6] Samsung, *Galaxy S10+ 1TB (Unlocked)* (2020).[7]

Cell phone capacity is extended even further by "cloud computing" and other remote access tools that allow users to "access data located elsewhere, at the tap of a screen." *Riley*, 573 U.S. at 397. For instance, every Apple device comes with iCloud storage of 5GB, but that can be expanded to as much as 2TB—four times the capacity of the highest-end iPhone currently on the market. Apple, *iCloud* (2020).[8] Any data from the device can be stored either locally or in the cloud—and deleted apps and associated data can be re-downloaded from the cloud with ease.

---

[3] https://www.apple.com/iphone/compare/.
[4] https://www.iclick.com/pdf/howbigisagig.pdf.
[5] https://www.apple.com/iphone/compare/.
[6] 1 Terabyte (TB) is 1064 Gigabytes (GB).
[7] https://www.samsung.com/us/mobile/phones/galaxy-s/galaxy-s10-plus-1tb-unlocked-sm-g975uckfxaa/.
[8] https://www.apple.com/icloud/.

The combination of local and cloud storage enables easy access on a cell phone to information and records relating to an astonishing amount of an individual's life. A phone's "capacity allows even just one type of information to convey far more than previously possible" in part because "the data on a phone can date back to the purchase of the phone, or even earlier." *Riley*, 573 U.S. at 375. The "retrospective quality of the data" gives border agents access to "information otherwise unknowable" and allows them to reconstruct a person's life. *Carpenter*, 138 S. Ct. at 2218.

The many different categories of data stored on a phone compounds the privacy interests. A cell phone "collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record." *Id*. Indeed, as technology gets "better and better at extracting meaning" from large data sets, it may "reveal things about us we did not expect others to know." Hal Abelson, Hen Ledeen, & Harry Lewis, *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion* 2 (2008).

Cell phones collect in one place such a wide range of data about an individual because of the vast number of apps consumers download and use on a regular basis. Apps "offer a range of tools for managing detailed information about all aspects of a person's life" that can "form a revealing montage of the user's

life." *Riley*, 573 U.S. at 396. For nearly any task, interest, or hobby, "there's an app for that." *Id.* at 396. The mere presence of an app icon on a phone can tell the viewer about the owner's political affiliation, *see, e.g.,* Fox News, *Fox News App* (2020);[9] Apple Store Preview, *Democracy Now!* (2020);[10] religion, *see, e.g.*, Apple Store Preview, *Daily Bible Inspirations* (2020);[11] App Store Preview, *Daily Quran Verse*s (2020);[12] or sexual orientation, *see, e.g.,* App Store Preview, Grindr (2020).[13] But the data created through use of an app reveals even more. The average American has over 100 apps installed on their phone, App Annie, *The State of Mobile 2019* at 13 (2019),[14] and spends an average of 226 minutes in apps on their cell phone a day, Mary Meeker, *Internet Trends 2019*, Bond, at 46 (June 11, 2019) [hereinafter Mary Meeker's Report 2019].[15]

Apps capture and store highly sensitive personal information. Almost 60% of Americans have downloaded a mobile health app. Paul Krebs & Dustin Duncan, *Health App Use Among US Mobile Phone Owners: A National Survey*, 3 JMIR

---

[9] https://www.foxnews.com/apps-products.
[10] https://apps.apple.com/us/app/democracy-now/id959877465.
[11] https://apps.apple.com/us/app/daily-bible-inspirations/id494789758.
[12] https://apps.apple.com/us/app/daily-quran-verses-inspirational-motivational-ayahs/id1001177285.
[13] https://apps.apple.com/us/app/grindr-gay-chat/id319881193.
[14] *Available at* https://www.appannie.com/en/insights/market-data/the-state-of-mobile-2019/.
[15] https://www.bondcap.com/report/itr19/#view/1.

mHealth and uHealth 101 (2015).[16] Health app data is extended by the use of wearable devices, such as watches and fitness trackers. Over a fifth of American adults regularly wear a smart watch or fitness tracker. Emily A. Vogels, *About One-in-Five Americans Use a Smart Watch or Fitness Tracker*, Pew Res. Ctr. (Jan. 9, 2020).[17] These wearable devices track a wide range of private information, including heart rate and location data. Sarah Silbert, *All the Things You Can Track with Wearables*, Lifewire (July 8, 2019).[18] There are also specialty wearables that monitor for certain events, such as a fertility bracelet that measures skin temperature, breathing rate, and heat loss. Ava, *How Ava Works* (2020).[19] Wearables then send the data they collect to an app on the users' cell phone. Health apps also allow users to manually enter data about their health and lifestyles. For instance, Apple's Health App can store a cell phone user's daily steps, meal habits, heart rate, reproductive health and sleep schedules, health records—including one's daily medication, immunization records, clinical vitals—and more. Amanda Capritto, *The Complete Guide to Apple's Health App*, CNET (Apr. 18, 2019).[20]

---

[16] *Available at* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4704953/.
[17] https://www.pewresearch.org/fact-tank/2020/01/09/about-one-in-five-americans-use-a-smart-watch-or-fitness-tracker/.
[18] https://www.lifewire.com/what-wearables-can-track-4121040.
[19] https://www.avawomen.com/how-ava-works/.
[20] https://www.cnet.com/health/the-complete-guide-to-apples-health-app/.

Health and activity apps are not the only applications that store a user's location data. Map programs, rideshare apps like Uber and Lyft, even photos store or encode location data. Fred Zahradnik, *How to Find Your Location History in Google Maps or iPhone*, Lifewire (Apr. 10, 2020);[21] Uber Guide, *How to Check Your Uber History* (2017);[22] Apple, *Browse Photos by Location on iPhone* (2020).[23] This historical location data is precisely the information *Carpenter* found to provide "an all-encompassing record of the holder's whereabouts," justifying heightened Fourth Amendment protection. 138 S. Ct. at 2217.

Mobile apps can also reveal detailed information about an individual's most intimate relationships, including their dating history. Thirty percent of Americans have used a dating site or app. Emily A. Vogels, *About Half of Never-Married Americans Have Used an Online Dating Site or App*, Pew Res. Ctr. (Mar. 24, 2020).[24] Among Americans aged 18 to 29, about half have used a dating app or site. Emily A. Vogels, *10 Facts About Americans and Online Dating*, Pew Res.

[21] https://www.lifewire.com/location-history-google-maps-iphone-1683392.
[22] https://www.uberguide.net/check-uber-history/.
[23] https://support.apple.com/guide/iphone/browse-photos-by-location-iph390138909/ios.
[24] https://www.pewresearch.org/fact-tank/2020/03/24/the-never-been-married-are-biggest-users-of-online-dating/.

Ctr. (Feb. 6, 2020).[25] Data in these apps can reveal a user's sexual orientation, relationships, communications, and more.

A cell phone can also reveal a user's video viewing habits. Americans are increasingly using their cell phones to watch movies, television shows, and other entertainment. Between 2017 and 2019, Americans spent 20% more sessions in video streaming apps such as Netflix. App Annie, *State of Mobile 2020* at 32 (2020).[26] These apps store a user's viewing history. Similar apps for books and audiobooks reveal a user's reading habits. *See, e.g.,* Apple Store Preview, *Kindle* (2020);[27] Audible, *Apps for Listening to Audible Audiobooks* (2020).[28]

Consumers also increasingly use their phones for banking and financial transactions. Eight out of ten consumers use mobile banking on a regular basis. Citi, *Mobile Banking One of Top Three Most Used Apps by Americans, 2018 Citi Mobile Banking Study Reveals* (Apr. 26, 2018).[29] The Chase app, for instance, allows phone users to view up to 24 months of transactions and up to seven years of credit card and bank statements. Chase, *Chase Mobile Banking* (2020).[30]

---

[25] https://www.pewresearch.org/fact-tank/2020/02/06/10-facts-about-americans-and-online-dating/.
[26] *Available at* https://www.appannie.com/en/go/state-of-mobile-2020/.
[27] https://apps.apple.com/us/app/amazon-kindle/id302584613.
[28] https://www.audible.com/howtolisten.
[29] https://www.citigroup.com/citi/news/2018/180426a.htm.
[30] https://www.chase.com/digital/mobile-banking.

Consumers continue to use their phones as communication devices. As cell phone users turn away from phone calls and towards text messages and emails, cell phone data will increasingly track and memorialize all conversations. Text messaging is the most widely- and frequently-used app. Aaron Smith, *U.S. Smartphone Use in 2015*, Pew Res. Ctr. (Apr. 1, 2015). Meanwhile, around 88% of Americans use email on their phones. *Id.* Notably, messaging platforms that offer encryption services, such as Telegram and Whatsapp, have outpaced the growth of non-encrypted messaging services, indicating the ever-increasing importance of personal privacy to consumers. Mary Meeker's Report 2019. In 2018, 87% of web traffic was encrypted, up from 53% in 2016. *Id.*

Social media use is also proliferating: 73% of US adults use YouTube, 69% use Facebook, 37% use Instagram, and 24% use Snapchat. Andrew Perrin & Monica Anderson, *Share of U.S. Adults Using Social Media, Including Facebook, Is Mostly Unchanged Since 2018*, Pew Res. Ctr. (Apr. 10, 2019).[31] For millennials, the numbers are even more striking: 91% use YouTube, 79% use Facebook, 67% use Instagram, and 62% use Snapchat. *Id.* Each app stores personal data, including private posts and direct messages, search histories, preferences, and more.

[31] https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/.

Cell phones do not just store personal data; they also contain sensitive business records. Almost 90% of companies expect their employees to use their cell phones for work purposes. Syntonic, *BYOD Usage in the Enterprise* (2016).[32] Additionally, while in the past, many workers had separate personal and professional cell phones, this is no longer the case. Only 26% of companies provide employees with work phones. Steelcase, *Engagement and the Global Workplace* (2016).[33] In contrast, 72% have a bring-your-own-device policy and actively encourage their employees to use personal devices for work purposes. Diane Garey, *BYOD and Mobile Security*, Tenable (Apr. 5, 2016).[34]

Law enforcement officers inspecting or searching a phone are likely to see sensitive information on the screen even if they don't open specific apps. Push notifications—messages from apps that pop up on a cell phone screen automatically—can display sensitive personal information about communications, transactions, and other activities. *See* Android, *Notifications Overview* (Dec. 27, 2019);[35] Apple, *Use Notifications on Your iPhone, iPad, iPod Touch* (2020).[36]

---

[32] https://syntonic.com/wp-content/uploads/2016/09/Syntonic-2016-BYOD-Usage-in-the-Enterprise.pdf.
[33] http://cdn2.hubspot.net/hubfs/1822507/2016-WPR/Americas/Final_Digital_PDF.pdf.
[34] https://www.tenable.com/blog/byod-and-mobile-security-2016-spotlight-report-results.
[35] https://developer.android.com/guide/topics/ui/notifiers/notifications.
[36] https://support.apple.com/en-us/HT201925.

Smartphones not only store and provide access to a wealth of sensitive personal data, they also authenticate access to other accounts: social media accounts, bank accounts, email accounts, and other profiles. For example, Apple built a password storage system into the iPhone. *See* Apple, *Set Up iCloud Keychain* (2020) ("iCloud Keychain remembers . . . your information—like your Safari usernames and passwords, credit cards, Wi-Fi passwords, and social log-ins—on any device that you approve.")[37] Several other apps store user login information for many sites and applications in one place. *See, e.g.*, Dashlane, *Features* (2020);[38] Zoho Vault, *Store and Organize Passwords* (2020);[39] LastPass, *LastPass Mac App* (2020).[40] This means that a user's online identities are all easily accessible to anyone who has access to their phone. Indeed, users might not be able to access their financial accounts or other essential services if they lose access to their cell phone. Matt Elliott, *Two-Factor Authentication: How and Why to Use It*, CNET (Mar. 28, 2017).[41]

Many apps will, by default, store your login information and never ask for the information again. For example, when a user logs into Facebook on their iPhone, the app will keep the user logged in by default and store the password.

---

[37] https://support.apple.com/en-us/HT204085.
[38] https://www.dashlane.com/features.
[39] https://www.zoho.com/vault/online-password-manager-features.html.
[40] https://helpdesk.lastpass.com/mac-app/.
[41] https://www.cnet.com/how-to/how-and-why-to-use-two-factor-authentication/.

Zack Whittaker, *Facebook Admits It Stored "Hundreds of Millions" of Account Passwords In Plaintext*, TechCrunch (Mar. 21, 2019).[42] Some social media apps, including Twitter and Facebook, require the user to take affirmative steps to log out. *See* Twitter, *How to Log Out of the Twitter App on an iOS Device* (2020);[43] Facebook, *How do I Log Out of the iPhone or iPad App?* (2020).[44]

Smartphones can also give law enforcement access—or even a view—into an individual's home. Home security systems allow users to monitor and control multi-camera systems from their phones. *See, e.g.,* Blink, *Blink Home Monitor App* (2020).[45] Blink, for instance, provides a live video feed from all of a user's home cameras, Blink, *How to Access Live View* (2020),[46] and also historical video footage, Blink, *How Can I View Motion Clips?* (2020).[47] Meanwhile, smart door locks provide an easy way to unlock the doors of a user's home with their smartphone and to monitor who is entering and leaving. *See* John R. Delaney, *The Best Smart Locks for 2020*, PCMag (Apr. 9, 2020).[48]

---

[42] https://techcrunch.com/2019/03/21/facebook-plaintext-passwords/.
[43] https://help.twitter.com/en/using-twitter/revoke-twitter-access-on-ios-app.
[44] https://www.facebook.com/help/ipad-app/112099682212213?helpref=uf_permalink.
[45] https://blinkforhome.com/blink-app.
[46] https://support.blinkforhome.com/using-the-blink-app/how-to-access-live-view.
[47] https://support.blinkforhome.com/using-the-blink-app/how-can-i-view-motion-clips.
[48] https://www.pcmag.com/picks/the-best-smart-locks.

B. The American Bar Association has recognized that searches of cell phones pose acute threats to both privacy and client confidentiality.

Attorneys, like the Plaintiff, have acute privacy interests in the contents of their cell phones because of the presence of confidential and protected attorney-client information. The American Bar Association ("ABA") recently called for a warrant requirement for border searches of electronic devices because of the substantial privacy and confidentiality interests at stake. Prior to their call for an across-the-board warrant requirement, the ABA had also recognized the unique impact that border searches have on attorney-client information. The ABA argued that the Department of Homeland Security ("DHS") should revise U.S. Customs and Border Protection ("CBP") and Immigrations and Customs Enforcement ("ICE") border search directives to require reasonable suspicion for an "advanced search," and should adopt special protocols for the handling of attorney devices. But the DHS has still not revised all of its border search policies. In 2019, the ABA adopted a resolution calling on the judiciary, Congress, and the DHS to require a warrant to search an electronic device at the border unless another warrant exception applied. Am. Bar. Ass'n, *Midyear Meeting 2019—House of Delegates Resolution 107A* (2019).[49]

---

49 https://www.americanbar.org/content/dam/aba/administrative/house_of_delegates/resolutions/2019-midyear/2019-midyear-107a.pdf.

In 2017, Linda A. Klein, President of the ABA, sent the DHS a letter calling on the Department to express "serious concerns regarding the standards that permit [CBP and ICE] officers to search and review the contents of lawyers' laptop computers, cell phones, and other electronic devices at U.S. border crossings without any showing of reasonable suspicion." Letter from Linda Klein, President, Am. Bar Ass'n, to Gen. John F. Kelly, USMC (Ret.), Sec'y of Homeland Sec., & Joseph B. Maher, Acting Gen. Counsel, Dep't of Homeland Sec. (May 5, 2017).[50] Klein declared that "just as border security is fundamental to national security, so too is the principle of client confidentiality fundamental to the American legal system." *Id*. at 1. The letter decried the fact that the CPB and ICE border search directives at the time led border officers and immigration agents to exercise "sweeping powers to search electronic devices at the border, with or without reasonable suspicion of any wrongdoing." *Id*. And while the directives required "special handling" for privileged and confidential legal documents, Klein stated that those provisions were "not sufficiently clear or comprehensive enough to protect" the rights of clients. *Id*. at 3. The letter called on DHS to revise its border search directives "to state that when a lawyer traveling across the border with a

[50] *Available at* https://www.americanbar.org/content/dam/aba/images/government_affairs_office/attyclientprivissue(bordersearchesofattorneydevices,abalettertodhs,finalversion,may5,2017).pdf.

laptop computer or other electronic device asserts that the device contains privileged or confidential client information, the device can be subjected only to a routine cursory physical inspection," and to require "a subpoena based on reasonable suspicion or a warrant supported by probable cause" to read, duplicate, seize, or share privileged or confidential electronic documents. *Id*. at 4.

In response to the ABA letter, DHS revised some of its directives, adopting the standard from the Ninth Circuit's decision in *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013), *cert. denied*, 561 U.S. 1156 (2014), that an "advanced search" of an electronic device requires reasonable suspicion. *See* U.S. Customs & Border Prot., CBP Directive No. 3340-049A (Jan. 4, 2018).[51] The new ABA president, Hilarie Bass, commented that the revised policy was "a clear improvement over the prior policy," but "more clearly needs to be done." Lee Rawles, *Traveling Lawyers Get New Protections in Device Searches at Border*, ABA Journal (Jan. 25, 2018).[52]

In 2019, the ABA adopted a policy that "urges the federal judiciary, Congress, and the Department of Homeland Security to enact legislation and adopt

---

[51] *Available at* https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border- Search-of-Electronic-Media-Compliant.pdf.

[52] http://www.abajournal.com/news/article/new_guidelines_for_electronic_device_searches_at_us_borders_will_impact_att.

policies to protect the privacy interests of those crossing the border by imposing standards for searches and seizures of electronic devices, protection of attorney-client privilege, the work product doctrine, and lawyer-client confidentiality." Am. Bar. Ass'n, *Midyear Meeting 2019—House of Delegates Resolution 107A* (2019). In particular, the ABA urged "the federal judiciary to recognize the substantial privacy and confidentiality interests, as well as the important national security and law enforcement interests, implicated by searches and seizures of electronic devices at the border." Am. Bar Ass'n, *Revised 107A* (2019). The ABA also urged that the DHS

- require a warrant based on probable cause for seizures (other than temporary seizures for searches other than forensic searches or for the purpose of obtaining a warrant) and forensic searches of electronic devices carried by American citizens and lawful permanent residents entering the country, or by any person leaving the country, unless an exception to the warrant requirement other than the border search exception applies;
- prohibit any government entity from denying an American citizen or lawful permanent resident entry or exit based on the person's failure to disclose an access credential or provide access to an electronic device for a search;

- fully protect the attorney-client privilege, the work product doctrine, and the lawyer's ethical obligation to maintain confidential information during border crossings; and
- require the federal government to record each instance in which it conducts a forensic search of an electronic device seized at the border and issue an annual report summarizing such searches.

Id.

Warrantless searches of attorney cell phones at the border raise acute privacy and confidentiality concerns. This Court should follow the ABA to require border and immigration officers obtain a warrant before searching an attorney's cell phone.

II. The government's interests in warrantless searches of cell phones at the border do not outweigh an individual's substantial privacy interest in the contents of their cell phone.

A. The traditional border search exception was justified by the government's interest in interdicting contraband and ascertaining the identity and citizenship of those seeking admission to the United States.

Professor Laura Donahue has traced the origins of both customs and immigration authorities to conduct warrantless searches at the border and identified two interests protected by the doctrine: interdicting contraband and ascertaining the identity and citizenship of individuals seeking entry to the United States. Laura K.

Donahue, *Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches*, 128 Yale L. J. F. 961-1015 (2019).

On the history of the customs authority, Professor Donahue notes that, in the earliest days of the republic, collection of duties justified warrantless searches at the border. Following independence, the United States needed revenue to pay for the war. Donahue at 974. Taxes on imported goods brought in revenue, but contraband meant a loss. *Id.* Thus, in 1789, Congress authorized customs officials to board any vessel "in which they shall have *reason to suspect* any goods, wares, or merchandise subject to duty shall be concealed; and therein to search for, seize, and secure any such goods, wares, or merchandise." An Act to regulate the Collection of the Duties imposed by law on the tonnage of ships or vessels, and on goods, wares and merchandises imported into the United States, ch. 5, § 24, 1 Stat. 29, 43 (1789) (codified at 19 U.S.C § 482) (emphasis added). If, however, an agent suspected that illegally imported materials were concealed in a "dwelling house, store, building, or other place," the agent had to obtain a warrant to conduct a search. *Id*. Congress continued to stress the importance of enforcing duties at the border in subsequent acts. Donahue at 975–77. Given this history, Professor Donahue compares the border search exception to the fleeing felon exception: "it was only in the hot pursuit of goods illegally brought into the country that broader powers could be exercised." Donahue at 984. Meanwhile, customs agents do not

have authority to open and inspect sealed mail unless it weighs more than sixteen ounces and there is reason to suspect the envelope contains one of only a few categories of objects. 19 U.S.C. § 1583.

The authority to search U.S. citizens for immigration purposes is even more tenuous. Immigration authorities focus on non-citizens seeking admission to the United States. *See, e.g.*, 8 U.S.C.A. § 1357(a). Once a U.S. citizen has identified themselves and presented proof of citizenship, immigration officials must produce a warrant to search the individual's cell phone. Donahue at 1013.

Professor Donahue's findings bring into focus the Supreme Court's analysis of the justifications underlying the border search exception. *See, e.g., United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985) ("Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country."); *Carroll v. United States*, 267 U.S. 132, 153–54 (1925) ("Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in"); *see also United States v. Molina-Isidoro*, 884 F.3d 287, 295 (5th Cir. 2018) (Costa, C.J., specially concurring) (reciting precedent supporting limited customs

authority to conduct warrantless searches). In short, the border search exception to the Fourth Amendment warrant requirement is not a general purpose waiver of all privacy rights at the border. The border search doctrine serves specific purposes and expanded warrantless search techniques should not be permitted if they are not justified by those purposes.

B. The justifications underlying the border search exception do not apply in the context of cell phones or are outweighed by an individual's interest in privacy.

The traditional rationales for the border search exception do not map on to the search of an American citizen's cell phones at the border. As the immigration interest does not apply at all in this case—Plaintiff is a U.S. citizen—this section focuses on CBP's authority to conduct a warrantless search of a cell phone.

In *Riley,* the Supreme Court found that extending the search incident to arrest exception to cell phone searches would "untether the rule from the justifications underlying" the exception: officer safety and preservation of evidence. *Riley,* 573 U.S. at 384–85, 86. The Court first noted that a cell phone could not be used as a weapon to threaten an officer's safety, and that the most extensive warrantless search that could be authorized pursuant to the officer safety justification was an examination of the "physical aspects" of the phone to ensure it did not conceal a weapon like "a razor blade between the phone and its case." *Id.* at 387. The Court then rejected the destruction of evidence justification because once

the officer secured the phone, there was little risk the arrestee could delete evidence. *Id*. at 388.

The interest in interdicting physical contraband similarly does not justify warrantless searches of cell phones. A brief physical examination can dispel any suspicion that a physical object is hidden within a phone. *See Molina-Isidoro*, 884 F.3d at 294-95 (Costa, C.J., specially concurring) ("the best argument for carving [cell phones] out of the government's traditional border-search authority is the physical limitations of their capacity"). Regarding digital analogues of physical objects that customs agents are authorized to interdict (e.g. national defense information and contraband images or files), the balance weighs in favor of the individual's privacy interest in their cell phone data.

Riley provides further guidance here. In *Riley*, the government suggested that it be able to search a cell phone incident to arrest for data with a pre-digital counterpart, such as a photograph or a bank statement, that an arrestee might have previously carried in their pocket. *Id.* at 400. The Court rejected this argument because of the amount of historical data a phone can access:

> The fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years.

Id. In the same way, pre-digital containers such as suitcases, backpacks, and pockets could only hold a limited number of photographs or other documents, not millions of pages of documents.

Digital searches are different than physical inspections. A brief physical search could reveal an object that might be contraband and provide evidence of whether the object is, in fact, contraband. There is no similar way to narrow a search of digital items without searching all of them. If border agents can search a phone for national defense information without a warrant, they will necessarily search *all* of the data on a phone: that information could be contained in photographs, text messages, Facebook messages, videos, audio, etc. A search for contraband images or files would similarly require searching every file—or, at the very least, every image file—on an electronic device, depending on the method customs officials use to conduct the search.

Searches for digital contraband thus would inevitably "expose to the government far *more* than the most exhaustive search of a house." *Riley*, 573 U.S. at 396. The initial weighing of interests that resulted in the pre-digital border search exception certainly did not account for exhaustive searches that would implicate millions of personal files and information traditionally only stored in the home. Indeed, as Professor Donahue points out, early customs laws explicitly required a warrant for searches of uncustomed and contraband goods in a home or

other building, signaling that customs agents could not violate the privacy of a home for such searches. Donahue at 1010–11. This history indicates that, in today's world where we carry more private information with us across the border than is present in the home, a warrant is needed to search for digital contraband on a cell phone.

Further diminishing the government's interest in warrantless searches for digital contraband at the border, digital contraband lacks any direct nexus to the border. In order for physical contraband to enter the United States, it must pass through customs and border control. The same is not true for digital contraband, which primarily enters the United States through the internet. Accordingly, law enforcement typically uses different methods to detect and locate digital contraband. Policing of child sexual exploitation materials ("CSEM"), for instance, is largely focused on electronic service providers ("ESPs"), many of which routinely scan their services for instances of known CSEM. *See* 18 U.S.C. § 2258A. Indeed, over 1,400 companies are registered to make CyberTipline reports to NCMEC, and 16.8 million of the 16.9 million reports of digital CSEM came from ESPs. Nat'l Ctr. for Missing & Exploited Child., *CyberTipline* (2020).[53] These types of cases typically are not initiated by and do not involve searches by border agents at ports of entry.

[53] https://www.missingkids.org/gethelpnow/cybertipline#bythenumbers.

There is also no justification for treating cell phones differently than the other small containers that routinely transit the border: mail envelopes. Customs officials are required to obtain a warrant or the consent of the sender or intended recipient to search sealed mail weighing sixteen ounces or less. 19 U.S.C. § 1583(d). As Professor Donahue points out, the equivalent to a sealed envelope in the digital world is a digital message sealed by a password or encrypted. Donahue at 1007. And, under *Riley* and *Carpenter*, the privacy interest in digital correspondence and communications is even stronger than physical mail because of the volume of information accessible from a cell phone. Thus, border agents should not be able to access encrypted and otherwise password-protected correspondence on electronic devices without a warrant.

C. Allowing warrantless searches for digital evidence at the border would provide no practical limit to cell phone searches.

The limited justification that underlies the border search exception—interdicting contraband and ascertaining the identity and citizenship of those seeking entrance to the United States—does *not* justify law enforcement efforts to "use the movement of people to look for evidence of criminal activity." Donahue at 963. That is the definition of a fishing expedition. Yet, the United States has argued that courts should expand the border search exception to include suspicionless searches for evidence of criminal activity. The Court should reject

this argument outright, just as the Supreme Court rejected the same argument in *Riley*. 573 U.S. at 398–99.

The Supreme Court has long distinguished between searches for contraband at the border and searches for evidence. "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." *Boyd v. United States*, 116 U.S. 616, 623 (1886). The difference was in historical authorization: since the colonial and founding eras, the law authorized seizure of contraband. *Id*. But "no similar tradition exists for unlimited authority to search and seize items that might help to prove border crimes but are not themselves instrumentalities of the crime." *Molina-Isidoro*, 884 F.3d at 297 (Costa, C.J., specially concurring).

In *Riley,* Chief Justice Roberts quoted Learned Hand for the observation that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." *Riley*, 573 U.S. at 396 (quoting *United States v. Kirschenblatt*, 16 F.2d 202, 203 (C.A.2)). Just because Americans now regularly carry all of that information in their phones whenever they cross the border does not erase their Fourth

Amendment protections. This Court should not extend the border search exception to evidence of criminality on a cell phone.

CONCLUSION

Amicus respectfully requests that this Court reverse the lower court's decision to deny Plaintiff summary judgment and a preliminary injunction.

Respectfully submitted,

*/s/ Alan Butler*_____
Alan Butler
Counsel of Record
Megan Iorio
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of 6,500 words of Circuit Rule 29.3 and Fe. R. App. P. 29(a)(5). This brief contains 6,483 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and Circuit Rule 32.1 and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word in 14-point Times New Roman style.

Dated: June 9, 2020

*/s/ Alan Butler*_____
Alan Butler
Counsel of Record
Megan Iorio
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

CERTIFICATE OF SERVICE

I hereby certify that on June 9, 2020, this brief was electronically filed with the Clerk of the Court for the United States Court of Appeals for the Fifth Circuit through the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Dated: June 9, 2020

*/s/ Alan Butler*_____

Alan Butler
Counsel of Record
Megan Iorio
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140