Case No. 19-10842

UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

BRIAN MATTHEW MORTON,

Defendant-Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS, FORT WORTH DIVISION
IN CASE NO. 19-CR-17-1, THE HONORABLE REED CHARLES O'CONNOR

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND ELECTRONIC PRIVACY INFORMATION CENTER IN SUPPORT OF DEFENDANT-APPELLANT

Jennifer Lynch
Counsel of Record
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993
jlynch@eff.org

Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004
Tel: (212) 549-2500

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Tel: (415) 373-0758

Alan Butler
Megan Iorio
Melodi Dincer
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Avenue NW
Washington, DC 20036
Tel: (202) 483-1140

Counsel for Amici Curiae

July 13, 2021

SUPPLEMENTAL CERTIFICATE OF INTERESTED PERSONS

Pursuant to this Court's Rule 28.2.1, the undersigned counsel of record for *amici curiae* certify that the following additional persons and entities 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.

1. The number and style of this case are *United States v. Brian Matthew Morton*, No. 19-10842.
2. ***Amicus Curiae*:** Electronic Frontier Foundation. The Electronic Frontier Foundation is a nonprofit organization recognized as tax exempt under Internal Revenue Code § 501(c)(3). It has no parent corporation and no publicly held corporation owns 10 percent or more of its stock.
3. **Counsel for *Amicus Curiae* Electronic Frontier Foundation**: Jennifer Lynch
4. ***Amicus Curiae***: American Civil Liberties Union. The ACLU is a nonprofit organization recognized as tax exempt under Internal Revenue Code § 501(c)(3). It has no parent corporation and no publicly held corporation owns 10 percent or more of its stock.
5. **Counsel for *Amicus Curiae* ACLU**: Jennifer Lynch, Jennifer Granick, and Brett Max Kaufman.
6. ***Amicus Curiae***: Electronic Privacy Information Center. EPIC is a nonprofit organization recognized as tax exempt under Internal

Revenue Code § 501(c)(3). It has no parent corporation and no publicly held corporation owns 10 percent or more of its stock.

7. **Counsel for *Amicus Curiae* EPIC**: Alan Butler, Megan Iorio, and Melodi Dincer.

Dated: July 13, 2021

/s/ Jennifer Lynch
Jennifer Lynch

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTEREST OF *AMICI CURIAE*[1]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles embodied in the Federal Constitution and our nation's civil rights laws. The ACLU has frequently appeared before courts, including this one, throughout the country in Fourth Amendment cases, both as direct counsel and as *amicus curiae*.

The Electronic Frontier Foundation ("EFF") is a member-supported, nonprofit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 30,000 active donors and dues-paying members across the United States. EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law to technology. EFF regularly participates both as direct counsel and as *amicus* in the Supreme Court, this Court, and other state and federal courts in cases addressing the Fourth Amendment and its application to new technologies.

The Electronic Privacy Information Center ("EPIC") is a public-interest research center in Washington, D.C. established to focus public attention on emerging privacy and civil liberties issues in the information age. EPIC

[1] No party's counsel authored this brief in whole or in part. Neither any party nor any party's counsel contributed money that was intended to fund preparing or submitting this brief. No person other than *amici*, their members, or their counsel contributed money that was intended to fund the preparing or submitting of this brief. All parties have consented to the filing of this brief.

participates as *amicus curiae* before courts across the country in cases involving constitutional rights and emerging technologies.

Amici have, alone or together, appeared as either counsel or *amicus* in the following cases: *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (cell-site location information); *Riley v. California*, 573 U.S. 373 (2014) (electronic device search incident to arrest); *United States v. Jones*, 565 U.S. 400 (2012) (warrantless GPS tracking); *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013) (abrogated by *Carpenter*, 138 S. Ct. 2206); *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (en banc) (delayed search of information seized pursuant to warrant for evidence of a different offense); *People v. Hughes*, 958 N.W.2d 98 (Mich. 2020) (similar); *Commonwealth v. Snow*, 160 N.E.3d 277 (Mass. 2021) (proper scope of warrant to search cell phone).

INTRODUCTION AND SUMMARY OF ARGUMENT

Cell phones today generate and store extremely revealing information about the people who use them. The Fourth Amendment protects those people's property and privacy rights in that information, both to shield the innocent from prying government eyes and also to prevent law enforcement from rummaging through vast amounts of information that could be assembled into a story of criminal conduct, even when the government lacked probable cause to suspect any criminal conduct in the first place. Here, the panel was wrong to find that the government had probable cause to search Mr. Morton's phone, because there was no reason to believe that evidence of the crime of drug possession would be found there. The mere fact that people, including those who possess drugs, use their phones to conduct their business, is insufficient to justify expansive government searches of vast amounts of private data.

The panel was correct, however, that the scope of cell phone searches must closely adhere to the probable cause showing, lest authority to search a device for evidence of one crime mutate into authority to search the entirety of the device for evidence of any crime—a prohibited general search. Courts have many options they can deploy to ensure that investigators do not conduct general searches. Here, there was an easy path—do not grant authority to search categories of data that there is no probable cause to believe will contain evidence of the crime under

investigation. The warrant should not have included "photographs," and the investigators should not have looked at photos because the affidavit did not support probable cause to believe that individuals in possession of drugs take pictures of themselves or otherwise preserve evidence as images.

ARGUMENT

I. CELL PHONES CONTAIN AN IMMENSE AMOUNT OF PRIVATE, SENSITIVE DATA

Smartphones are ubiquitous, highly portable devices that "place vast quantities of personal information literally in the hands of individuals." *Riley v. California*, 573 U.S. 373, 386 (2014). Americans use their phones for a wide variety of purposes and, as a result, smartphones contain a voluminous and varied collection of data. While data is often organized by application or file type, even discrete categories of information, alone or in combination with each other, comprise a "digital record of nearly every aspect of [our] lives." *Id.* at 375.

Cell phone use is now deeply entrenched in the fabric of daily life. Ninety-seven percent of Americans own a cell phone and 85% own a smartphone specifically.[2] These devices are "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. Mobile devices have become the screen that people access first and most often.[3] Nearly half of

[2] Pew Rsch. Ctr., *Mobile Fact Sheet* (Apr. 7, 2021), https://www.pewinternet.org/fact-sheet/mobile/.

[3] John Koetsier, *We've Spent 1.6 Trillion Hours on Mobile So Far in 2020*, Forbes (Aug. 17, 2020), https://www.forbes.com/sites/johnkoetsier/2020/08/17/weve-spent-16-trillion-hours-on-mobile-so-far-in-2020/.

Americans check their smartphones as soon as they wake up in the morning.[4] People proceed to spend an average of four hours a day using various apps on their phones.[5] Cell phone use is so persistent that the medical field has adopted a term to describe the intense anxiety many people experience when they fear being separated from their cell phones: *NOMOPHOBIA: NO MObile PHone PhoBIA*.[6]

Americans' dependency on smartphones has, intentionally and inadvertently, resulted in our phones containing vast troves of our personal information. Indeed, cell phones "differ in both a quantitative and a qualitative sense" from other objects because of "all [the personal information] they contain and all they may reveal." *Riley*, 573 U.S. at 393, 403. The "immense storage capacity" of smartphones allows them to function as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers," and to store extensive historical information related to each functionality. *Id.* at 393. Because a cell phone "collects in one place many distinct types of information,"—for example, an address, a note, a prescription, a bank

---

[4] Diane Thieke, *Smartphone Statistics: For Most Users, It's 'Round-the-Clock' Connection*, ReportLinker (Jan. 26, 2017), https://www.reportlinker.com/insight/smartphone-connection.html.

[5] App Annie, *The State of Mobile 2021* at 7 (2021), https://www.appannie.com/en/go/state-of-mobile-2021/.

[6] Sudip Bhattacharya et al., *NOMOPHOBIA: NO MObile PHone PhoBIA*, 8 J. Family Med. Prim. Care 1297 (2019), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6510111/.

statement, or a video—those types of information "reveal much more in combination than any isolated record," *id.* at 394, and they reveal much more about "an individual's private interests or concerns." *Id.* at 395.

Cell phones collect a wide range of data about individuals through the millions of applications people download and regularly use. In 2020, the average smartphone user had forty apps installed on their phone.[7] Apps "offer a range of tools for managing detailed information about all aspects of a person's life," and the information generated by those apps "form[s] a revealing montage of the user's life." 573 U.S. at 396. For example, about one in five Americans currently track information related to their personal health through their mobile devices.[8] Wearable devices, such as smart watches and heart rate monitors, collect additional health data, much of which is accessible via an app on the user's cell phone. Wearables can capture sensitive information like heart rates, location data, skin temperature, breathing rate, heat loss, and fat composition, and are sometimes used to track deeply personal events such as fertility or menstruation cycles.[9] Further,

---

[7] Nick Gallov, *55+ Jaw Dropping App Usage Statistics in 2021*, TechJury (July 4, 2021), https://techjury.net/blog/app-usage-statistics.

[8] Justin McCarthy, *One in Five U.S. Adults Use Health Apps, Wearable Trackers,* Gallup (Dec. 11, 2019), https://news.gallup.com/poll/269096/one-five-adults-health-apps-wearable-trackers.aspx.

[9] Sarah Silbert, *All the Things You Can Track with Wearables*, Lifewire (Dec. 2, 2020), https://www.lifewire.com/what-wearables-can-track-4121040/; Geoffrey A. Fowler & Heather Kelly, *Amazon's New Health Band Is the Most Invasive Tech We've Ever Tested*, Wash. Post (Dec. 10, 2020),

apps connected to "smart" home security systems allow users to monitor and control multicamera systems from their phones, providing access to individuals' most intimate physical spaces.[10] The very presence of certain dating apps can signal a person's sexual orientation, and the data collected by such apps can reveal even more information about intimate relationships and communications.[11] People are also increasingly using their phones for banking and financial transactions, with roughly 76% of Americans using their primary bank's mobile app for everyday banking tasks within the last year.[12] And people continue to use their phones as communication devices, with encrypted messaging platforms outpacing non-encrypted messaging services, indicating a desire for personal privacy.[13]

---

https://www.washingtonpost.com/technology/2020/12/10/amazon-halo-band-review/.

[10] *See, e.g.*, Blink, *Blink Home Monitor App* (2020), https://blinkforhome.com/blink-app.

[11] *See, e.g.*, App Store Preview, *Grindr* (2021), https://www.grindr.com/; App Store Preview, *Kinkoo* (2021), https://www.kinkoo.app/.

[12] Mitch Strohm, *Digital Banking Survey: 76% of Americans Bank Via Mobile App—Here Are the Most and Least Valuable Features*, Forbes (Feb. 24, 2021), https://www.forbes.com/advisor/banking/digital-banking-survey-mobile-app-valuable-features/.

[13] Mary Meeker, *Internet Trends 2019*, Bond at 168 (June 11, 2019), https://www.bondcap.com/report/itr19/; Jack Nicas et al., *Millions Flock to Telegram and Signal as Fears Grow Over Big Tech*, N.Y. Times (Jan. 13, 2021), https://www.nytimes.com/2021/01/13/technology/telegram-signal-apps-big-tech.html.

A typical smartphone today will reveal even more about a person than a *Riley*-era phone because of increased storage capacity. Storage capacities increase every year, as does the sheer volume of personal data stored on—and accessible from—cell phones. In 2014, when the Supreme Court decided *Riley*, the top-selling smartphone could store sixteen gigabytes of data. *Id.* at 394.[14] The minimum storage on Apple's current line of iPhones is sixty-four gigabytes.[15] That is over one million Word documents, almost 40,000 photos, 32 full-length movies, and almost 15,000 songs.[16] Some Android models offer one terabyte of storage, roughly sixty-four times more than a *Riley*-era phone.[17]

A cell phone's storage capacity allows "even just one type of information to convey far more than previously possible." *Riley*, 573 U.S. at 394. For example, access to just the photos on a person's phone allows "[t]he sum of [their] life [to be] reconstructed through a thousand photographs labeled with dates, locations, and descriptions." *Id.* Access to that person's text messages amounts to accessing

[14] Sixteen gigabytes equals about 3,680 songs, 8,672 digital copies of *War and Peace*, 9,520 digital photos, or eight feature-length movies. *See* iClick, *How Big is a Gig?* (2013), https://www.iclick.com/pdf/02_howbigisagig_infographic.pdf.

[15] Apple, *Compare iPhone Models* (2021), https://www.apple.com/iphone/compare/.

[16] iClick, *supra* note 14.

[17] Samsung, *Galaxy S10+ 1TB (T-Mobile)* (2021), https://www.samsung.com/us/business/products/mobile/phones/galaxy-s/galaxy-s10-plus-1tb-t-mobile-sm-g975uckftmb/.

"a record of all [their] communications" over long periods of time, as "the data on a phone can date back to the purchase of the phone, or even earlier" when users sync information in the cloud. *Id.* And access to a single payment app on their phone can reveal to whom they sent money, when, and for what purposes, also revealing that individual's intimate social relationships.[18]

Given cell phones' vast storage capacity, the variety of apps users have on their phones, and the detailed data contained in each of those apps, cell phones produce "a digital record of nearly every aspect of [users'] lives—from the mundane to the intimate." *Riley,* 573 U.S. at 395. While a single app or type of data can reveal an extraordinary amount about a person, the combination of the many different types of data on a phone can essentially reconstruct a person's life.

II. THE FOURTH AMENDMENT REQUIRES THAT POLICE DEMONSTRATE PROBABLE CAUSE TO SEARCH A CELL PHONE AND THE DATA IT CONTAINS

It is axiomatic that officers must have probable cause to support the search of a cell phone. *See generally Riley*, 573 U.S. 373. Further, probable cause to search or seize *some* data on the phone cannot justify access to the totality of the phone's contents. Given the vast amounts of personal data stored on phones and all

[18] *See* Ryan Mac et al., *We Found Joe Biden's Secret Venmo. Here's Why That's A Privacy Nightmare For Everyone.*, Buzzfeed News (May 14, 2021), https://www.buzzfeednews.com/article/ryanmac/we-found-joe-bidens-secret-venmo.

that can be gleaned from that data, as discussed above, strict limits on searches and seizures are necessary to preserve privacy. To prevent unreasonable cell phone searches, law enforcement must specifically identify the information they have probable cause to search, and must only search that information. Otherwise, the immense amounts of personal data stored on most cell phones today will be subject to unconstitutionally overbroad searches.

In this case, officers failed to follow constitutionally required limitations. First, they failed to show probable cause in the affidavit sufficient to support a search of the phone itself. The facts of this case—an arrest for simple drug possession—do not support probable cause to search Mr. Morton's phone at all. And second, even if there were probable cause to support a search of *some* data on the phone, the affidavit did not demonstrate that any evidence would be stored in the form of photographs.

A. Especially in the context of digital data searches and seizures, warrants must be based on probable cause, be particularized, and avoid overbreadth.

To safeguard our constitutional rights, courts must apply Fourth Amendment law stringently to address the unique attributes of digital data, ensuring that police direct their searches of electronic data towards evidence for which there is probable cause and away from voluminous, intimate, non-responsive private information.

The Fourth Amendment was enacted to prevent general searches, *Groh v. Ramirez*, 540 U.S. 551, 561 (2004), and to prevent the government from engaging in a "general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). To accomplish this goal, the Fourth Amendment requires that warrants be supported by probable cause to believe that a crime was committed and that evidence of the crime will be found in the place to be searched or the thing to be seized. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Law enforcement must demonstrate "a nexus . . . between the item to be seized and [the] criminal behavior" under investigation. *United States v. Griffin*, 555 F.2d 1323, 1325 (5th Cir. 1977) (quoting *Warden v. Hayden*, 387 U.S. 294, 307 (1967)); *Kohler v. Englade*, 470 F.3d 1104, 1109 (5th Cir. 2006). Warrants must also particularly describe the things to be searched and seized. Through these fundamental limitations, properly drafted warrants prevent overbroad searches and cabin officer discretion in conducting searches or seizures.

Like personal computers, cell phones are able to "store and intermingle a huge array of one's personal papers in a single place." *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009). This increases the risk that law enforcement will, after seizing a digital device, be able "to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important." *Id.*; *see also Stanford v. Texas,* 379 U.S. 476, 511–12

(1965) (The "constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain."). To prevent every cell phone search from turning into a general search, courts must rigorously adhere to the Fourth Amendment's probable cause requirement, both for the phone itself and for the data stored on it.

B. Contrary to the panel opinion, facts supporting probable cause to believe that a suspect is guilty of drug possession do not automatically provide probable cause to search a phone.

In this case, the magistrate judge issued, and the panel approved, a warrant to search Mr. Morton's cell phone based on the officer's training and experience that people in possession of drugs must acquire them from somewhere, and that it is likely that evidence of that transaction exists on the cell phone. (ROA.269-270) (in the officer's experience, people use cell phones "to arrange for the illicit receipt and delivery of controlled substances"). While officers' training and experience can often help form a basis for probable cause, there nevertheless must be some specific connection to the investigation underway, and not a general assertion that would apply to any and all such crimes. *See Gates*, 462 U.S. at 239 ("wholly conclusory statement" in affidavit is insufficient to support probable cause); *Rivera v. Murphy*, 979 F.2d 259, 263–64 (1st Cir. 1992) (officer's "bald assertion that based on his 'observations, training and experience,' he had probable cause to

make the arrest" without "facts to support his legal conclusion" was insufficient); *State v. Baldwin*, 614 S.W.3d 411, 417 (Tex. App. 2020) (en banc), *petition for discretionary review granted* (Tex. 2021) (explaining why "generic, boilerplate language" about suspects' cell phone use is insufficient to establish probable cause). Yet the panel held that, if evidence of a crime is often found in a particular location, that constitutes probable cause to believe that such evidence will be found in that location in the specific case at issue. *United States v. Morton*, 984 F.3d 421, 427 (5th Cir. 2021), *reh'g en banc granted and opinion vacated*, 996 F.3d 754 (5th Cir. 2021). Were the panel correct, law enforcement could obtain a warrant to seize and search cell phones in essentially every case. Such a result would undermine *Riley* and the Supreme Court's recognition that cell phones, "with all they contain and all that they may reveal," hold "the privacies of life." *Riley*, 573 U.S. at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

The panel's conclusion is also contrary to precedent. Compare this case to that of other unlawful possession cases. Drug dealers often keep controlled substances in their homes, purses, or cars, but police are not generally permitted to search these places without investigation-specific reasons to believe evidence will be found in those places. *See, e.g., United States v. Brown*, 828 F.3d 375, 382 (6th Cir. 2016) (no probable cause to search home where affidavit contained no evidence that Brown distributed narcotics from his home, used it to store narcotics,

or that any suspicious activity had taken place there); *cf. United States v. Broussard*, 80 F.3d 1025, 1034-35 (5th Cir. 1996) (upholding search warrant where affidavit was based on officer training and experience because affidavit also contained facts linking the residence to drug trafficking); *In re Search of Cellular Telephone Towers*, 945 F. Supp. 2d 769, 770–71 (S.D. Tex. 2013) (affidavit demonstrated nexus between the records sought and the criminal activity being investigated where there was evidence that the subject used a cell phone during and in furtherance of the offense).

For similar reasons, police are not permitted to search drug suspects' cell phones in every case. *See, e.g., United States v. Lyles*, 910 F.3d 787, 794–95 (4th Cir. 2018) (affidavit that phone was inside a home where officers found "three marijuana stems in the trash" provided insufficient cause to search the phone); *In re Search of a White Apple iPhone, Model A1332*, 2012 WL 2945996, *2 (S.D. Tex. 2012) (affidavit insufficient where government failed to establish nexus between the targeted cell phone and violation of sex-offender registration requirement, and application "seem[ed] more designed to seek evidence that the defendant may have violated statutes regarding child pornography").

A number of state courts have rejected similar warrants where the only fact offered to support probable cause was the officer's "training and experience" that people, including criminals, use their phones and computers to communicate. As

the Massachusetts Supreme Judicial Court noted in *Commonwealth v. White*, this allegation alone is insufficient. 59 N.E.3d 369, 375 (Mass.2016). "If this were sufficient . . . it would be a rare case where probable cause to charge someone with a crime would not open the person's cellular telephone to seizure and subsequent search." *Id.* at 591–92 (citing *Riley*, 573 U.S. at 399 (only an "inexperienced or unimaginative law enforcement officer . . . could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone")); *see also*, *e.g.*, *State v. Castagnola*, 46 N.E.3d 638, 654 (Ohio 2015) (magistrate judge may not infer "online" activities merely because search for information was conducted by people of a certain age, nor do text messages admitting criminal activity equal probable cause to search a computer); *Wheeler v. State*, 135 A.3d 282, 288 (Del. 2016) (warrant to search a computer may not be based on boilerplate language reciting qualifications and experience of investigators without further justification why evidence of witness tampering would be found on a device); *State v. Keodara*, 364 P.3d 777, 783 (Wash. 2015), *review denied*, 185 Wash.2d 1028 (2016) (warrant affidavit alleging drug dealers keep records about their transactions on phones provided insufficient probable cause to search); *State v. Mansor*, 81 P.3d 930 (Or. 2016), *aff'd*, 421 P.3d 323 (Or. 2018) (warrant lacked probable cause where investigating officer, based on training and experience, sought information from a suspect's computer preceding the time period relevant

to the offense).

The government's application to search Mr. Morton's phone, based only on a general assertion that people who take drugs may communicate over their phones to acquire them or discuss them, (*see* ROA.269-70), was constitutionally insufficient.[19] Without a specific reason to believe evidence related to the crime charged existed on the phone in *this* case, the investigators had no probable cause to have searched Mr. Morton's phone in the first place.

C. Here, the government needed separate probable cause to search each of the categories of information found on the cell phone.

Even if there were probable cause to search Mr. Morton's cell phone for evidence, the government could only have looked at folders and files on the device for which there was reason to believe evidence may be found. This means that, before searching texts, photographs, or emails, the government has to show that the evidence is likely to be in the form of a text, photograph, or email. Here, the government did not demonstrate a nexus between photographs and criminal behavior. Therefore, the warrant should not have included "photographs," and the investigators should not have examined them.

[19] There are many ways to procure drugs other than by text message, such as asking a friend in person, calling a drug dealer from a pay phone or landline, or loitering meaningfully on a corner.

The need for particularity and for probable cause to search each category of information found on the phone is well-grounded in Fourth Amendment jurisprudence and, contrary to the government's arguments, emphatically reinforced by the Supreme Court in *Riley*. Probable cause requires law enforcement to "know if specific information is contained on a device [before] searching it," and it cabins searches of that data to those designed to uncover evidence of a specific crime.[20] If law enforcement can "search the entire electronic haystack for the needle" and "may see all the information the [entire] haystack reveals along the way," then a warrant for all data on a phone is no different than a general warrant.[21] Of course, Fourth Amendment-required limitations will always be context-specific. For example, even where police are lawfully in a home, police cannot open a spice box when searching for a rifle. *See, e.g.*, *Horton v. California*, 496 U.S. 128, 141 (1990). Nor can they rummage through a medicine cabinet while looking for a flat-screen television. *See, e.g.*, *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013). This basic principle is not defeated simply because potential evidence is digital rather than physical.

[20] Orin Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech. L. Rev. 1, 3 (2015).
[21] *Id.*; *see also id*. at 10-11 (describing such searches as "perilously like the regime of general warrants that the Fourth Amendment was enacted to stop").

The government argues that the panel's holding to this effect conflicts with *Riley*. (*Pet. of the U.S. For Rehearing En Banc* at 10-11 ("U.S. *En Banc* Petition"). But *Riley* does not support the conclusion that *all* the data on a phone can be searched so long as there is a warrant for the phone. To the contrary, *Riley* explicitly discussed the invasiveness of law enforcement access to different "categories," "areas," "types" of data, and "apps." *Riley*, 573 U.S. at 395, 396, 399. The Court also pointed out that electronic searches are categorically different from physical ones, and potentially result in extreme privacy intrusions. *See, e.g.*, *id.* at 395 ("certain types of data are also qualitatively different"). Primary among the reasons the Supreme Court gave for its holding in *Riley*—that to search a cell phone seized incident to arrest, police needed to "get a warrant," *id.* at 403—was the need to limit officer's unbridled access to the information stored on the phone. Justifications for search, whether arrests or warrants, do not give "police officers unbridled discretion to rummage at will among a person's private effects." *Id*. at 399 (citing *Arizona v. Gant*, 556 U.S. 332, 345 (2009)). In other words, the lesson of *Riley* is exactly what the panel in this case said it was: "distinct types of information, often stored in different components of the phone, should be analyzed separately." *Morton*, 984 F.3d at 425.

Indeed, with increasing frequency, courts have followed *Riley* to hold that looking in the right place, not *every* place, is the only plan that makes sense and

complies with the Constitution. *See, e.g., Burns v. United States*, 235 A.3d 758, 775 (D.C. 2020) (warrant authorizing search for categories of data for which there was no probable cause was "constitutionally intolerable"); *People v. Musha*, 131 N.Y.S.3d 514 (N.Y. Sup. Ct. 2020) (in child abuse case, there was probable cause to search the phone's photographs, but not to examine web search history); *State v. McLawhorn*, 2020 WL 6142866, *24–*26 (Tenn. Crim. App. 2020) (cannot search entirety of phone to determine whether device has flashlight function); *State v. Bock*, 485 P.3d 931, 936 (Or. App. 2021) (warrant authorizing the search of a cell phone for circumstantial evidence about the owner and any evidence related to suspected criminal offenses including unlawful firearm possession was not sufficiently specific under constitution).

For example, the Tenth Circuit Court of Appeals has held that investigators may only search files for evidence related to the probable cause showing. *United States v. Carey*, 172 F.3d 1268, 1271-73 (10th Cir. 1999). In *Carey*, a police officer, pursuant to a warrant, searched a laptop for evidence of drug distribution. While searching the laptop, the officer discovered child sexual abuse material (CSAM). At this point, he began searching for and opening files he believed were likely to contain CSAM, instead of continuing to search only for evidence of drug distribution. *Id.* at 1273. The Tenth Circuit held that searching the computer data for evidence of a crime for which there was no probable cause was an

"unconstitutional general search" and violated the suspect's expectation of privacy in data not described in the warrant. *Id*. at 1276; s*ee also In re United States of America's Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius*, 770 F. Supp. 2d 1138, 1147–1151 (W.D. Wash. 2011) (application to search and seize "all electronically stored information . . . contained in any digital devices seized from [defendant's] residence for evidence relating to the crimes of copyright infringement or trafficking in counterfeit goods" was improper because it sought "the broadest warrant possible," and did not propose to use a search technique that foreclosed the plain view doctrine's application to digital materials). By contrast, in *United States v. Walser*, which had facts similar to those in *Carey*, the investigator, upon unexpectedly finding child abuse images, "immediately ceased his search of the computer hard drive and . . . submit[ted] an affidavit for a new search warrant specifically authorizing a search for evidence of possession of child pornography." 275 F.3d 981, 984–985 (10th Cir. 2001). Because the officer did not search images without demonstrating to a judge a nexus to the crime he was investigating, the Tenth Circuit concluded that the materials were properly admitted into evidence. *Id*. at 987. As these cases demonstrate, even when there is probable cause to search a device for *something*, data that is not connected to the probable cause showing may not be accessed or examined absent a further warrant.

And in *People v. Herrera*, the Colorado Supreme Court suppressed evidence contained in a text message involving a third party not named in the warrant. The court held that the government's argument that *any* text message folder could be searched because of the abstract possibility that the folder might contain indicia of who owned the phone, or might have been deceptively labeled, would result in an unconstitutional limitless search. 357 P.3d 1227, ¶¶ 18, 35 (Colo. 2015). In *State v. Henderson*, the warrant permitted a search of "[a]ny and all information' contained on the cell phone." 854 N.W.2d 616, 633 (Neb. 2014). There, the Nebraska Supreme Court relied on *Riley* to find that the warrants were insufficiently particular because they did not refer to the specific crime being investigated. *Id.* at 633. The law is clear that police cannot get a warrant to search, nor search, information for which there is no probable cause, so a magistrate judge must reject search warrant applications asking for "all-data" on the phone without making the requisite showing. *See also, e.g.*, *In re Search of Black iPhone 4*, 27 F. Supp. 3d 74, 79 (D.D.C. 2014).

Applying these principles, this case is straightforward. The issuing magistrate judge should have limited the warrant to specific categories of data, and the investigators should not have searched outside of those categories; photographs should have been off-limits.

Certainly, limiting searches by category of document will not always be possible. But that is no justification for discarding the Fourth Amendment's probable cause and particularity requirements. In fact, courts have a number of options depending on the facts of the case. For example, warrants can protect against searches for evidence of past crimes as well as against broad searches justified by probable cause for minor crimes. *Riley*, 573 U.S. at 399 (warrant necessary for this purpose). Warrants can do this by specifically imposing date range limits. For example, in *State v. Mansor*, the Oregon Supreme Court held that the warrant to search the defendant's computer should have been limited to search history on the day of a child's injury and death, not the weeks and months before the death, as the government requested. 421 P.3d 323, 343–44 (Or. 2018) (interpreting Article I, section 9 of the Oregon Constitution). Similarly, in *Commonwealth v. Snow*, the Massachusetts Supreme Judicial Court found that a warrant to search the cell phone of a defendant accused of murder was insufficiently particular because it authorized a search without a temporal limit, even though the government argued "it was unknown 'when the weapon used was acquired and when any related conspiracy may have been formed.'" 160 N.E.3d 277, 288 (Mass. 2021); *see also People v. Thompson*, 178 A.D.3d 457, 458 (N.Y. App. Div. 2019) (warrant to search defendant's phones without a time limitation did not satisfy the Fourth Amendment's particularity requirement).

Beyond category and date limitations, warrants can establish search protocols that limit the documents examined based on keywords or other search parameters, or magistrate judges can ask for search logs facilitating a post-execution review. Courts can require independent review teams to segregate relevant from irrelevant information. Courts can also impose use restrictions, as the Oregon Supreme Court did in *Mansor*, 421 P.3d at 326, or limit application of the plain view doctrine. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1179 (9th Cir. 2010) (en banc) (Kozinski, C.J., concurring); *Bock*, 485 P.3d at 938. Depending on the circumstances of the case, there are a number of tools that can ensure that the government examines no more data than is required to accomplish a probable cause-based search.

The government's petition for rehearing *en banc* relies heavily on the argument that the panel misunderstood photographs on Mr. Morton's phone to be "places" when actually they are "things." U.S. *En Banc* Petition at p. 1, 8 ("[T]he panel's novel rule . . . confuses the "place to be searched" (the cell-phone) with the "things to be seized" (contacts, call logs, text messages, photographs)"). But it does not matter if photographs and the folders in which they are stored are "things" or "places." *Mansor*, 421 P.3d at 338 ("[T]he state's semantic observation that a computer is literally a 'thing' is a truism that does not compel a legal conclusion."). As discussed above, the Fourth Amendment requires probable cause

to seize or search papers and effects—things—just as well as places. Authorization to search a place does not equal permission to seize or examine any or all things inside that place. *See Arizona v. Hicks*, 480 U.S. 321 (1987) (officers legitimately searching a home in connection with a shooting may not also examine stereo components to access serial numbers not in plain view); *United States v. Garcia*, 496 F.3d 495 (6th Cir. 2007) (warrant to search entirety of house for cocaine did not permit search for or seizure of documents).[22]

In any case, a phone can be one place that nevertheless contains many other "places," just as a home is one place that also contains other places, such as a kitchen, a bedroom, and a garage. And a place such as a home contains objects one might describe as "things" that can also be searched, like footlockers and purses. The police must have probable cause to examine each of those things, even if they are inside a place for which there is a valid warrant to search. Officers must have independent probable cause to search folders and documents stored on a phone, regardless of whether the government describes each folder or file as a "place" or a "thing." Exactly the same, authorization to search Mr. Morton's cell phone did not convey equal permission to examine all the places *or* things—folders, documents,

[22] Courts often analogize from physical world experience to understand digital world phenomena. These analogies are almost always inexact, and multiple analogies can be drawn, each of which could lead to a different conclusion. Here, the Court need grapple with none of these ambiguities.

or photographs—stored there.

In the government's rehearing petition, it takes a quote from *Riley* out of context to argue for exactly the result that the Supreme Court was trying to protect against: unbridled access to digital information for which there is no probable cause. U.S. *En Banc* Pet. at p. 10 (asserting that *Riley*'s comment that "officers would not always be able to discern in advance what information would be found where on a cell phone" means that law enforcement does not need to identify in advance categories of documents, files, or folders subject to search (quoting *Riley*, 573 U.S. at 399 (quotation marks omitted))). However, that quote from *Riley* does not support the government's argument. In context, the government in *Riley* argued that it should be allowed to access information with certain meaning—information relevant to the crime, the arrestee's identity, or officer safety—regardless of where or how it was stored. *Id.* at 399. The Supreme Court rejected this solution as "impos[ing] few meaningful constraints on officers" in part because permission for this type of search would "sweep in a great deal of information," especially given that officers could not know where the information would be found. *Id*. Indeed, this quote supports the *Appellant's* position that searches must be constrained, not the government's position to the contrary.

Despite the government's dire warnings about the consequences of the panel's analysis, there is nothing dangerous or radical about ensuring that

government searches of digital information comply with the longstanding principles enshrined in the Fourth Amendment that are intended to limit government authority and guarantee an active role for the judiciary. Documenting the government's reasons for searching a particular private place has been a bedrock requirement since the founding. Moreover, today's investigators have substantial tools for locating relevant information stored on a cell phone.[23] The practical reality is that no investigator can look at *everything* on a phone, because there is too much data. Investigators can employ technology, or even human discretion, in a manner reasonably calculated to find evidence of the crime under investigation. The Fourth Amendment dictates that warrants draw these bounds.

CONCLUSION

For the reasons stated above, this court should reverse the panel's opinion finding that there was probable cause to search Mr. Morton's cell phone. In the

[23] *See* Logan Koepke, et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*, Upturn (Oct. 2020), https://www.upturn.org/reports/2020/mass-extraction. Forensic tools can be far more discriminating than the government says. But even if the government described them correctly, the only reason that companies would sell such inferior tools is because the government is willing to buy them. The science required for comprehensive search is well-developed and already deployed in innumerable and publicly-available tools, such as e-discovery software, email search, image search, and the like. Forensic software companies can and will make a better tool for searching cell phones if their primary customer, the government, needs it. It would be a poor Constitution indeed that blessed the government's actions merely because the government did not pressure its forensic software providers to design better tools.

alternative, it should affirm the opinion's holding that there was no probable cause to search photographs on the device and that it unconstitutional for the government to have done so.

Dated: July 13, 2021

Respectfully submitted,

By: /s/ Jennifer Lynch
Jennifer Lynch

ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993
jlynch@eff.org

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Tel: (415) 373-0758

Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004
Tel: (212) 549-2500

Alan Butler
Megan Iorio
Melodi Dincer
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Avenue NW
Washington, DC 20036
Tel: (202) 483-1140

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(A)

I hereby certify as follows:

1. The foregoing Brief of *Amici Curiae* complies with the type-volume limitation of Fed. R. App. P. 32(a) or Fed. R. App. P. 28.1 because this brief contains 6,279 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) 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 Word 365, the word processing system used to prepare the brief, in 14 point font in Times New Roman.

Dated: July 13, 2021

/s/ Jennifer Lynch
Jennifer Lynch

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeal for the Fifth Circuit by using the appellate CM/ECF System on July 13, 2021. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: July 13, 2021

/s/ Jennifer Lynch
Jennifer Lynch