No. 23-2342

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

DONTAE LAMONT HUNT,

Defendant-Appellant.

On Appeal from the United States District Court
for the District of Oregon, Portland
D.C. No. 3:18-cr-00475-IM-1
The Honorable Karin J. Immergut, U.S. District Judge

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION, ACLU OF OREGON, ELECTRONIC FRONTIER FOUNDATION, ELECTRONIC PRIVACY INFORMATION CENTER, AND NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

Andrew Crocker
Hannah Zhao
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993
andrew@eff.org

Jake Wiener
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, D.C. 20036
Tel: (202) 483-1140
wiener@epic.org

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
425 California Street, 7th Floor
San Francisco, CA 94111
Tel: (415) 343-0758
jgranick@aclu.org

Nathan Freed Wessler
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel: (212) 549-2500
nwessler@aclu.org

Kelly Simon
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF OREGON
P.O. Box 40585
Portland, OR 97240
Tel: (503) 444-7015
ksimon@aclu-or.org

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 and 29(a)(4)(A) of the Federal Rules of Appellate Procedure, amici state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

Dated: May 31, 2024

/s/ Jennifer Stisa Granick
Jennifer Stisa Granick

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

STATEMENT OF INTEREST OF AMICI CURIAE[1]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to defending the civil liberties and civil rights guaranteed by the federal and state constitutions. The ACLU of Oregon is the ACLU's Oregon affiliate. The protection of privacy as guaranteed by the Fourth Amendment is of special concern to each organization.

The Electronic Frontier Foundation ("EFF") is a nonprofit organization that has worked for more than thirty years to protect privacy, free speech, and civil liberties in the digital world. EFF, with its over 30,000 active donors, represents the interests of technology users in court cases and broader policy debates surrounding the application of law in the digital age. EFF has served as amicus curiae in the Supreme Court in many cases addressing the intersection of the Fourth Amendment and new technologies, including those particularly involving or implicating cell phones. *See Carpenter v. United States*, 585 U.S. 296 (2018); *Riley v. California*, 573 U.S. 373 (2014); *United States v. Jones*, 565 U.S. 400 (2012).

[1] No counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than the amici curiae or their counsel made a monetary contribution intended to fund the brief's preparation or submission. Defendant, through his counsel, has consented to filing of this brief. The government consented to the filing, conditioned on our compliance with the requirements of Fed. R. App. P. 29 and with local Ninth Circuit rules and existing applicable scheduling orders.

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 and civil liberties issues. EPIC routinely participates as amicus curiae in cases concerning emerging privacy issues, new technologies, and constitutional interests. EPIC has authored several briefs specifically concerning searches of cell phones and personal data generated by cell phones. *See, e.g.*, Brief of Amicus Curiae EPIC, *O.W. v. Carr*, No. 23-1191, 2024 WL 776751 (4th Cir. May 18, 2023) (arguing that, under *Riley*, the school administrative search doctrine should not apply to cell phones in joint school and law enforcement searches); Brief of Amici Curiae EPIC et al., *Carpenter*, 585 U.S. 296 (arguing that the Fourth Amendment protects against warrantless seizure and search of location data); Brief of Amici Curiae EPIC et al., *Riley*, 573 U.S. 373 (arguing that warrantless search of a cell phone incident to an arrest is impermissible).

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands of direct members, and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL has filed numerous amicus briefs in the

Supreme Court on issues involving digital privacy rights, including in *Carpenter*, 585 U.S. 296; *Riley*, 573 U.S. 373; and *Jones*, 565 U.S. 400.

INTRODUCTION

As cell phones' storage capacity continues to expand, and as the data that users may store on their phones becomes more sensitive, detailed, and revealing, this Court should make clear that the "abandonment doctrine" does not apply to data stored on cell phones. In this case, that means that Defendant-Appellant has standing to challenge the search of the black iPhone, because he did not lose an expectation of privacy in the data stored on the device merely by virtue of having lost control of the device itself.

Cell phones have become "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 573 U.S. 373, 385 (2014). In *Riley*, the U.S. Supreme Court recognized that the ubiquity of cell phones, combined with their capacity to hold vast quantities of detailed personal information—potentially the "sum of an individual's private life"—make cell phones so qualitatively and quantitatively different from people's pre-digital property as to require a warrant to search one incident to an arrest. *Id*. at 394.

This appeal asks this Court to address whether Defendant-Appellant retained a Fourth Amendment–protected expectation of privacy in the data stored on a black

iPhone, even if the phone itself is properly considered abandoned.[2] The district court assumed that facts suggesting that the black iPhone had been physically abandoned meant that Defendant-Appellant had abandoned the data on the phone as well. *United States v. Hunt*, No. 3:18-cr-00475-IM, 2022 WL 1153985, at *3 (D. Or Apr. 19, 2022). Relying on pre-digital cases, the court therefore concluded that the owner of an abandoned phone no longer has a privacy interest in information stored on the phone. *Id*. (citing *Abel v. United States*, 362 U.S. 217, 241 (1960) and *United States v. Jackson*, 544 F.2d 407, 409 (9th Cir. 1976)).

Yet, the Supreme Court has made clear that "[w]hen confronting new concerns wrought by digital technology, [courts must be] careful not to uncritically extend existing precedents." *Carpenter v. United States*, 585 U.S. 296, 318 (2018). Because the district court's conclusion is inconsistent with the Supreme Court's holding in *Riley* and with subsequent Fourth Amendment cases, this Court should hold that the abandonment doctrine does not apply to data stored on electronic devices.

The same principles supporting *Riley*'s requirement of a warrant to search a cell phone incident to arrest apply equally to a phone found unattended by the police. It is one thing to seize the device. It is a separate matter to search the data stored on

[2] Amici express no opinion on whether the device itself should be considered abandoned under the facts of this case.

it. Courts must not treat cell phones, which are unique, like any other item of property. Even outside its owner's possession, a phone—unlike other property—is likely to contain "[t]he sum of an individual's private life." *Riley*, 573 U.S. at 394.

The Court should hold that owners of cell phones maintain an expectation of privacy in the contents of phones outside their immediate possession. This Court's prior panel decision in *United States v. Fisher*, 56 F.4th 673 (9th Cir. 2022), is not to the contrary. In *Fisher*, this Court concluded that defendants, by abandoning their phones, "lost any reasonable expectation of privacy in them, and lacked standing to seek suppression of the devices' contents." *Id.* at 688. However, it did so without considering whether the data stored on the phone should be treated differently from the physical phone itself. Neither party in that case presented any argument about the special protections courts have recognized for data on cell phones. Indeed, neither the defendants nor the panel cited *Riley* a single time.

Since *Riley* was decided in 2014, the number of Americans who own smartphones has nearly doubled, the storage capacity of modern cell phones has quintupled, and the average smartphone owner has at least twice as many apps on their phone.[3] The case for a warrant requirement to search cell phone data is even

[3] *Compare Riley*, 573 U.S. at 396 (describing various apps and noting, at that time, that the average smart phone user "has installed 33 apps, which together can form a revealing montage of the user's life."), *with* App Annie, *Spotlight on Consumer App Usage Part 1*, at 6 (2017), https://perma.cc/R82W-KBVD (assessing that the

stronger today. Absent some case-specific exception, such as consent, defendants should always have standing to challenge searches of the stored data from a cell phone, even if the phone is truly "abandoned." The Supreme Court's preference for "clear guidance" and "categorical rules" that are readily applied in the context of searches and seizures strongly supports a categorical warrant requirement to search the contents of an abandoned phone. *Riley*, 573 U.S. at 398.

ARGUMENT

I. Cell Phones and Similar Electronic Devices Contain Vast Amounts of Highly Personal Information, Making them Categorically Different from Other Physical Property.

A. Cell phone data reveals sensitive and intimate information about a person's life.

As of 2023, there were almost 8.9 billion mobile phone subscriptions worldwide.[4] The vast majority of Americans—97%—now own a cell phone of some kind. Nine in ten own a smartphone.[5] "Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went

---

average smartphone user in 2017 interacted with "over 30 apps per month," and had two to three times as many apps installed on their device).

[4] N*umber of Mobile (Cellular) Subscriptions Worldwide from 1993 to 2023*, Statista (Feb. 7, 2024), https://perma.cc/6H3T-8YBV.

[5] Pew Rsch. Ctr., *Mobile Fact Sheet* (Jan. 31, 2024), https://perma.cc/6V8R-WXUR; *cf*. *Riley*, 573 U.S. at 385 (citing Aaron Smith, *Smartphone Ownership 2013*, Pew Rsch. Ctr. (June 5, 2013), https://perma.cc/Y4A6-8ZF4 (noting "56% of American adults are now smartphone owners")).

about their day. Now it is the person who is *not* carrying a cell phone, with all that it contains, who is the exception." *Riley*, 573 U.S. at 395 (emphasis added).

The Supreme Court recognized in *Riley* that cell phones differ both quantitatively and qualitatively from physical objects and containers. *Id.* at 393. The sheer volume of information available on cell phones makes them fundamentally different from any pre-digital counterpart. With their "immense storage capacity," cell phones and similar electronic devices can contain the equivalent of "millions of pages of text, thousands of pictures, or hundreds of videos." *Id.* at 393–94. The minimum capacity of most smartphones today—at 128 GB[6]—is eight times as large as when the Court decided *Riley* just eleven years ago. *Id*. at 394 ("current top-selling smart phone has a standard capacity of 16 gigabytes"). And some phones today contain as much as one terabyte of in-built storage—enough space for hundreds of feature-length films.[7] As 5G technology becomes more widely adopted, this number

[6] Kerry Wan, *The Best Phones for 2024: Expert Tested*, ZDNet (Apr. 18, 2024), https://perma.cc/FP9Z-6VNY ("Most smartphones have a base storage capacity of 128 GB . . . ."); Brady Wang, *Smartphone Storage Capacity Zooms on Increased Demand*, Counterpoint (Apr. 19, 2021), https://perma.cc/F9EN-3246 (". . . 128GB is becoming the minimum standard for storage capacities in the mid-end to high-end segment.").

[7] *See, e.g.*, *How the Galaxy S24 Ultra Compares*, Samsung, https://perma.cc/4W2B-FU2R; *Compare iPhone Models*, Apple, https://perma.cc/L95P-NBVK; *How Much Is 1TB of Storage*?, Dropbox, https://perma.cc/7FV5-HVV3 ("One terabyte gives you the option of storing roughly: 250,000 photos . . . 250 movies or 500 hours of HD video . . . [or] 6.5 million document pages.").

will continue to increase because high-capacity storage enhances the experience of "high-speed communication, AI technology, AR/VR, and high-definition/4K content."[8]

Cell phones differ qualitatively from other types of property as well. They "collect[] in one place many distinct types of information . . . that reveal much more in combination than any isolated record." *Riley*, 573 U.S. at 394. Americans downloaded 12.6 billion apps in 2023 and spent an average of 4.5 daily hours interacting with their smartphones.[9] These apps can generate vast and varied data, including call logs, emails, text messages, voicemails, browsing history, calendar entries, contact lists, shopping lists, notes, diaries, photos and videos, books read, TV shows and movies watched, financial and health data, purchase history, dating profiles, metadata, and so much more. This information, in turn, can reveal an individual's most intimate thoughts and closely held secrets including political affiliations, religious beliefs and practices, sexual and romantic life, financial status, health conditions, and family and professional associations. *See Riley*, 573 U.S. at 394–96. Additionally, "[h]istoric location information is a standard feature on many

[8] Sujeong Lim, *Average Storage Capacity in Smartphones to Cross 80GB by End-2019*, Counterpoint (Mar. 16, 2019), https://perma.cc/67YL-U6MK; Federica Laricchia, *Penetration Rate of 5G Smartphones Worldwide from 2020 to 2027*, Statista (Feb. 13, 2024) , https://perma.cc/LB4P-WDCB.

[9] Data.ai, *State of Mobile 2024*, at 12–13 (2024), https://www.data.ai/en/go/state-of-mobile-2024/.

smartphones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Id.* at 396 (citing *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

Today's electronic devices enable the reconstruction of "the sum of an individual's private life" covering a lengthy amount of time—"back to the purchase of the [device], or even earlier." *Id.* at 394. While people cannot physically "lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read," they now do so digitally. *Id.* at 393. A cell phone not only "contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Id.* at 396–97.

B. People lose their phones all the time, and cell phone data is not lost even when the phone is.

Despite the fact that the data stored on cell phones is comprehensive, voluminous, revealing, and detailed, cell phone owners frequently get separated from their devices. According to the electronic device insurance provider Asurion,

Americans lost 4.1 million cell phones in 2022 alone—that's more than 11,000 phones each day, or 459 every hour.[10]

Modern cell phones allow users to store personal information in the "cloud"—that is, not on the devices themselves, but on servers accessible via the Internet.[11] Ubiquitous and seamless cloud storage means that smartphone users can easily and automatically back up the contents of their devices, such as photos, videos, contacts, and other data.[12] This allows people to maintain access to their files if their phone is damaged, lost, or stolen, by easily downloading the backed-up data to a new device.[13] As a result, losing or abandoning a physical phone often does not mean

---

[10] *What to Do If Your Phone Is Lost or Stolen*, Asurion, https://perma.cc/8CT3-Z69E; *Cf.* Calla Dietrick, *Smartphone Thefts Drop as Kill Switch Usage Grows*, Consumer Reports (June 11, 2015), https://perma.cc/9Z4F-ERKB (reporting the finding that in 2014, Americans lost around 3.1 million phones, with another 2.1 million phones stolen).

[11] *See* Peter Mell & Timothy Grance, Nat'l Inst. of Standards & Tech., Spec. Pub. No. 800-145, *The NIST Definition of Cloud Computing* (Sept. 2011), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[12] *See, e.g.*, *Back Up Your Device*, Google One Help, https://perma.cc/258L-2GL6 ("You can automatically back up your mobile device with Google One. If you backup your device, you can have another copy of your photos, videos, contacts, and other items in the cloud."); *Backup Methods for iPhone, iPad, and iPod Touch*, Apple, https://perma.cc/4WX5-2J87 ("iCloud backups include all the information and settings stored on your device that don't already sync to iCloud."); *Samsung Cloud*, Samsung, https://perma.cc/PLH8-RRDC.

[13] *E.g.*, *Back Up Your Device*, Google One Help, *supra* note 12 ("To get your data back when you get a new device, restore from your backup.").

losing or abandoning the data stored on it, which the user can still access through a secure cloud storage account.

For many cell phone users, cloud service is significant also because it allows them to automatically and instantaneously synchronize information across multiple devices. For example, a user may take a photo with their iPhone in the morning. The image is automatically uploaded to Apple's iPhoto cloud service. Midday, the user edits the photo on their laptop. That evening, they show their children the photo on an iPad tablet. Although the user has created the image with a phone, they have accessed the photo on three separate devices, and each time, Apple automatically records the user's actions and updates the image in conformity with their latest activity.[14]

The vast majority of Americans can access the same content they carry in their phones from at least one other device. Eighty-three percent percent of Americans own at least one laptop or desktop computer, tablet, or wearable computer in addition

[14] Depending on how an app or browser is designed and configured, copies of cloud data often are also temporarily stored or cached on the device itself. *See* Lee Bell, *What Is Caching and How Does it Work?*, Wired (May 7, 2017), https://perma.cc/DFA6-9XPV.

to a phone.[15] The average American household contains nearly six such devices.[16] When users have multiple devices storing and accessing the same data, the devices themselves become secondary. In fact, because so much data on a phone is also saved in the cloud, and in light of the ubiquity of device insurance to replace lost phones,[17] people who lose their phones often will not have the same need to urgently track it down as they would for an non-digital object like a briefcase or wallet.

Cloud-stored data could include personal email, banking records, and social media. It would be a vast and unwarranted expansion of the abandonment cases if merely losing one's phone meant a person was deemed to have abandoned all privacy and property interests in this data, even though they retain access, control, ownership, and privacy interests in that same data when it is stored in the cloud.

---

[15] Alexus Bazen, *Cell Phone Statistics 2024*, Consumer Affairs (Kristen Schmitt ed. Sept. 28, 2023, updated Dec. 12, 2023), https://perma.cc/7HZU-FQ87 (citing Jennifer Chan, *Multiple Device Ownership Means More Smartphone Usage*, Kantar, tbl.1 (Sept. 23, 2021), https://perma.cc/UDN8-5UU8).

[16] *Id.*

[17] *See, e.g.*, *Phone Insurance*, Asurion, https://perma.cc/GR8Z-5YLL; *Asurion Protection Plans: What Are They, and Do You Need One?*, CNET (Oct. 6, 2023), https://perma.cc/4T2C-VLVC (device insurance company Asurion has 280 million customers).

C. The fact that most phone users lock their device is a sufficient, but not necessary, sign that people consider cell phone data private even when they have lost control of the device.

In recognition of the sensitivity of information on phones and the ease with which the devices can be lost, most phone users—83%—report locking their phones.[18] However, facility with screen lock protections varies widely with age, with people with people over 65 leaving their phones unprotected at more than three times the rate of people ages 18–29.[19] This does not mean that older people do not care about the data on their phones. Rather, irrespective of whether the phone is protected by a passcode or biometric screen lock, people regard the information on their phones to be highly private.[20]

Although some courts have suggested that Fourth Amendment rights could turn on whether the phone user has enabled a passcode or biometric lock on the phone,[21] such a contingent rule would create tension with the Supreme Court's

---

[18] Colleen McClain et al., *How Americans View Data Privacy*, Pew Rsch. Ctr. (Oct. 18, 2023), https://perma.cc/RNH9-FFJP.

[19] *Id.*

[20] Mallory Newall & Johnny Sawyer, *A Majority of Americans Are Concerned About the Safety and Privacy of their Personal Data*, Ipsos (May 5, 2022), https://perma.cc/BX9V-PUPS (citing polling indicating that 84% of Americans are concerned about the safety and privacy of personal data).

[21] *See State v. K.C.*, 207 So. 3d 951, 958 (Fla. Dist. Ct. App. 2016) ("[T]he abandonment exception does not apply to cell phones whose contents are protected by a password."); *see also United States v. Guerrero-Torres*, 762 F. App'x 873, 875 n.1 (11th Cir. 2019) (reserving question "whether the contents of a password-

preference for bright-line rules that are easily administrable by police. *Riley*, 573 U.S. at 398 (proposal to require warrant for some cell phone searches but not others "contravenes our general preference to provide clear guidance to law enforcement through categorical rules"). The better rule is to require a warrant to search the contents of a cell phone deemed abandoned, at least absent unequivocal case-specific indication that the phone's user actually intended to abandon the contents of the phone. *E.g.*, *United States v. Guerrero-Torres*, 762 F. App'x 873, 876 (11th Cir. 2019) (defendant's decision to provide law enforcement with his passcode demonstrated that he did not expect to "guard the privacy of [his] phone's contents").

Given cell phones' "immense storage capacity" and vast collection of varied, sensitive, and revealing data, it is no wonder that the U.S. Supreme Court has held that people retain an expectation of privacy in cell phone–stored data such that a warrant is generally required to search the information stored on a phone, even when the device itself is lawfully seized without a warrant. *Riley*, 573 U.S. at 393.

---

protected cellphone can be abandoned."); *Wiltz v. State*, 595 S.W.3d 930, 935 (Tex. App. 2020) (in applying abandonment doctrine to search of phone, noting lack of "evidence that the cell phone was password-protected").

II. The Fourth Amendment "Abandonment Doctrine" Should Not Apply to Information Stored on Cell Phones Because Private Data Is Unlike Physical Property in Abandonment Case Law.

A. A pre-digital doctrine allowing warrantless searches and seizures cannot be mechanically applied to searches of digital data.

It was error for the district court to hold that when Defendant-Appellant abandoned his physical device, the black iPhone, he also relinquished his expectation of privacy in any information stored on the device. *Hunt*, 2022 WL 1153985, at *3 ("Defendant has no standing to object to the seizure and search of the black iPhone because Defendant lacked a reasonable expectation of privacy in the black iPhone—evinced through his abandonment of it.").

As the Supreme Court recognized in *Riley*, cell phones have no true equivalent in the pre-digital world. For that reason, the Court unanimously rejected the government's "strained" attempt to analogize searches of cell phones incident to arrest to searches of physical items—like a pack of cigarettes—which the Court had approved decades earlier. *See* 573 U.S. at 396–97; *id*. at 393–94 (discussing *United States v. Robinson*, 414 U.S. 218 (1973)).

The Supreme Court has consistently refused to mechanically extend older doctrines in ways that risk letting new technologies "shrink the realm of guaranteed privacy" under the Fourth Amendment. *Kyllo v. United States*, 533 U.S. 27, 34 (2001). For example, in *Kyllo* the Court declined to expand holdings from cases like *California v. Ciraolo*, 476 U.S. 207, 213 (1986), which said that people have reduced

or no expectations of privacy in matters visible without trespassing on private property, when it found intimate details inside the home were protected even though police were able to "see" those details from a public vantage point using thermal imaging technology. *Kyllo*, 533 U.S. at 33. Similarly, in *Jones*, a majority of justices recognized that police invaded a person's privacy interest in their movements when using a GPS device to pervasively track a car traveling on "public thoroughfares," despite the Court's earlier holding permitting police to tail a suspect for a short period using rudimentary radio beeper tracking technology in *United States v. Knotts*, 460 U.S. 276, 281 (1983). *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *id*. at 430 (Alito, J., concurring in the judgment). And in *Carpenter*, the Court refused to extend the "third party doctrine," developed in cases like *Smith v. Maryland*, 442 U.S. 735 (1979), to location data held by third-party phone carriers, despite the fact that the third-party carriers collected and retained the data. *Carpenter*, 585 U.S. at 309. In each of these cases, the Court has recognized that automatically extending case law from a different era involving less intrusive and revealing technologies to novel contexts would improperly erode Fourth Amendment protections.

The touchstone of these cases is the recognition that "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure [ ] preservation of that degree of

privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 585 U.S. at 305 (quoting *Kyllo*, 533 U.S. at 34) (alteration in original). Because newer technologies like thermal imaging, GPS trackers, and smartphones provide the government with an ability to execute previously impossible invasions of privacy at minimal cost and effort, applying the Fourth Amendment's warrant requirement is crucial to avoid leaving people "at the mercy of advancing technology." *Id.* Prior to the cell phone age, people never expected that police searching an arrestee would have direct access to a vast quantity of that person's communications, contacts, and personal records. *Riley*, 573 U.S. at 395. In the same way, no one could have imagined that a search of the contents of an abandoned item—a jacket, a billfold, a purse, even a briefcase—would lay bare all the intimate material that a cell phone contains. The logic of abandonment cases dealing with limited searches of physical items simply does not "extend[] to the qualitatively different category" of information at issue here. *Carpenter*, 585 U.S. at 309.

B. Under the abandonment cases, people do not manifest intent to abandon their cell phone data merely by virtue of having abandoned their physical device.

The Supreme Court has articulated the contours of what is frequently referred to as the "abandonment doctrine" through several cases, the most recent of which was *California v. Greenwood*, 486 U.S. 35, 40 (1988). In *Greenwood*, the Court held

that people have no reasonable expectation of privacy in garbage left out for collection because they have knowingly exposed their trash to any member of the public. *Id.*; *see also Abel*, 362 U.S. at 239 (warrantless seizure of the items in question was permitted only because the suspect "*chose* to leave some things behind in his [hotel] room, which he *voluntarily* relinquished." (emphases added)). Under this theory, police can conduct a warrantless seizure or search of an abandoned item because the owner has intentionally relinquished an expectation of privacy and a possessory interest in the object.

Abandonment is primarily a question of intent, so courts "must consider the totality of the circumstances to determine whether an individual, by their words, actions, or other objective circumstances, so relinquished their interest in the property that they no longer retain a reasonable expectation of privacy in it at the time of its search or seizure." *United States v. Baker*, 58 F.4th 1109, 1118 (9th Cir. 2023). Considering the realities of modern cell phone and device usage discussed above, the mere fact that police deem a cell phone to be abandoned does not mean that a phone's owner intended to abandon their privacy interest in the voluminous and diverse data stored on it.

Indeed, in related contexts, courts have held that even when the government has lawfully seized or collected an electronic device, a warrant is required to conduct subsequent searches of the data stored on it. *E.g. Riley*, 573 U.S. 373; *see also, e.g.*,

United States v. Ganias, 755 F.3d 125 (2d Cir. 2014) (requiring investigating agents to obtain a new warrant before searching computer hard drives that had been lawfully seized pursuant to an earlier warrant), *rev'd on other grounds*, 824 F.3d 199 (2d Cir. 2016) (en banc); *United States v. Galpin*, 720 F.3d 436, 446–47 (2d Cir. 2013); *United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999). Courts have applied the same principle in other areas where privacy interests are high. *E.g. Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602, 616, 618 (1989) (the "collection and subsequent analysis of . . . biological samples must be deemed [separate] Fourth Amendment searches" because "[t]he ensuing chemical analysis of the sample to obtain physiological data is a further invasion of the tested [individual's] privacy interests"); *United States v. Davis*, 690 F.3d 226, 246 (4th Cir. 2012) (permitting warrantless seizure of blood-stained clothing from hospital room under the plain-view exception, but requiring warrant for DNA testing of the clothing).

Yet the district court's finding of abandonment in this case is based solely on facts suggesting that the *device* was abandoned, without consideration of the different factors showing a person's deep and ongoing attachment to the *data*. The court below cited cases involving abandonment of physical objects, including a backpack and a baggie of suspected cocaine. *Hunt*, 2022 WL 1153985, at *3 (citing *United States v. Kelly*, No. 4:20-CR-00191-DCN, 2021 WL 2109189, at *4 (D. Idaho May 25, 2021) (backpack); *United States v. Woodson*, No. CR 11-00531

WHA, 2011 WL 5884913, at *8 (N.D. Cal. Nov. 23, 2011) (baggie)). But those examples lack the characteristics of individuals' ongoing connection to the information on their cell phones—a device that "hold[s] for many Americans 'the privacies of life'"—even if the device is lost. *Riley*, 573 U.S. at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

The facts that the district court interpreted as indicia of abandonment are difficult to square with the importance and sensitivity of the contents of phones and the fact that people often back them up to the cloud. People do not necessarily lose their data when they lose their phones, because they can access Internet-stored copies. A court would need much more than the fact of loss or abandonment of the physical phone to find an intent of its owner to intentionally abandon years' worth of private correspondence, intimate photos, family videos, financial information, and more. Indeed, properly seen, a phone is essentially a *means* to access a user's private data. In that way, it is like a housekey. But the district court would surely have seen the folly in concluding that losing, and then legally abandoning, one's keychain means that they forfeited a privacy interest in the contents of their house.

The concerns the Court enunciated in *Riley* with respect to law enforcement searches of cell phones incident to arrest apply with at least the same force to searches of abandoned devices. For the same reasons that "technology now allows an individual to carry such information in his hand," it also increases the likelihood

that devices containing the "privacies of life" will be misplaced or fall into unintended hands. *Id.* at 403. Mobile devices are small, are carried everywhere people go, and are easily dropped or left behind by mistake. Especially because phones are so easily misplaced, this Court should be wary of setting rules that risk underprotection of the sensitive data they contain. *See State v. Valles*, 925 N.W.2d 404, 410 (N.D. 2019) ("[A]n individual's privacy interest in a cell phone remains high even when it is lost.").

III. Neither This Court's Prior Cases Nor Decisions from Other Courts Support Dispensing with the Warrant Requirement Here.

Courts have so far been divided about whether the abandonment doctrine applies to data stored on cell phones. While some have concluded that the doctrine does apply, none of those opinions—including one from a prior panel opinion of this Court—is binding here. And because the logic underlying those decisions is flawed and fails to consider Supreme Court precedent on the unique sensitivity of cell phones, those decisions do not support the government's position.

Several months after the district court's denial of the motion to suppress below, a panel of this Court in a different case found that two defendants had abandoned cell phones they had left for nine months in the attic of a house they had sold. *Fisher*, 56 F.4th at 686–88. The panel focused on the question whether the defendants intended to abandon the physical phones. *Id.* Although the panel concluded in a single summary sentence that "[b]ecause Defendants abandoned the

devices, they lost any reasonable expectation of privacy in them, and lacked standing to seek suppression of the devices' contents," *id.* at 688, it provided no discussion or analysis whatsoever about whether the defendants' interest in the data stored on the phones differed from their interest in the physical phones themselves. That makes sense, as the defendants made no such argument in their brief, claiming only that they "did not intend to abandon the *devices*." Appellants' Joint Opening Brief 27, *Fisher*, 56 F.4th 673, 2022 WL 619287 (emphasis added).

The party presentation principle that is central to "our adversarial system of adjudication" means that "courts normally decide only questions presented by the parties." *United States v. Sineneng-Smith*, 590 U.S. 371, 375–76 (2020) (cleaned up). This Court should be careful not to overread *Fisher* when the panel in that case was not presented with, and did not address, the arguments about Fourth Amendment interests in the *contents* of phones advanced by Defendant-Appellant in this appeal.

Moreover, *Fisher*'s conclusion conflicts with an earlier statement from this Court, where a panel noted that under *Riley*, police were "definitely required" to obtain a warrant to search an abandoned phone. *United States v. Artis*, 919 F.3d 1123, 1127–28 (9th Cir. 2019). And in yet another (albeit unpublished) opinion, this Court has contemplated that even when a device is abandoned, the data may not be. *United States v. Zacherle*, 689 F. App'x 467, 468 (9th Cir. 2017). In *Zacherle*, the defendant had abandoned his computer, but this Court still briefly considered the

defendant's argument that "the files on his computer were entitled to greater protection than the computer itself." *Id.* The panel ultimately found that the defendant did not have an additional privacy interest in his files because neither the computer nor the files were locked, meaning he "exhibited no greater concern for the files [the computer] contained." *Id.*[22]

Other courts have similarly recognized that the question of continuing expectation of privacy in the data on a device is separate from whether there was abandonment of the device itself. In *State v. K.C.*, 207 So. 3d at 958, a Florida appeals court held that the abandonment doctrine does not apply to the contents of cell phones protected by a passcode because a passcode demonstrates an intent to keep data private. And in *Richardson v. State*, 282 A.3d 98 (Md. 2022), the Maryland Supreme Court indicated that a cell phone search may require a warrant or warrant exception, even if the physical phone has been abandoned. Although officers secured a warrant to search one of the abandoned phones, the court did not assume that the defendant lacked standing to challenge the cell phone search just because he abandoned a backpack containing the phone itself. Instead, the court analyzed whether the warrant for the cell phone search met the particularity requirement or whether the good-faith exception applied. *Id.* at 106, 113–26. In doing so, the court

[22] As explained above, *supra* Part I.C, the rule this Court sets in this case should not turn on whether a screen lock or password protection is enabled at the time a purportedly abandoned device is discovered by police.

implied that the defendant retained his privacy interest in the phone's contents despite abandoning the physical container holding the phone.

In a similar analysis, the Eleventh Circuit also recognized that someone may retain a privacy interest in the contents of their abandoned device. *Guerrero-Torres*, 762 F. App'x at 875. The court found that the defendant had no standing to challenge the search of his phone data, not because the phone was abandoned, but because he "failed to establish a subjective expectation of privacy in the contents of his phone" by giving law enforcement his password. *Id*.

These opinions support the conclusion that the abandonment doctrine does not apply to cell phone data.

CONCLUSION

For the foregoing reasons, this Court should hold that the abandonment doctrine does not apply to cell phone data, and reverse the district court's opinion.

Dated: May 31, 2024

Respectfully submitted,

/s/ Jennifer Sitsa Granick

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
425 California Street, 7th Floor
San Francisco, CA 94111
Tel: (415) 343-0758
jgranick@aclu.org

Counsel for Amici Curiae

Nathan Freed Wessler
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel: (212) 549-2500
nwessler@aclu.org

Kelly Simon
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF OREGON
P.O. Box 40585
Portland, OR 97240
Tel: (503) 444-7015
ksimon@aclu-or.org

Andrew Crocker
Hannah Zhao
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993
andrew@eff.org

Jake Wiener
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, D.C. 20036
Tel: (202) 483-1140
wiener@epic.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I certify as follows:

1. This Brief of Amicus Curiae the Electronic Frontier Foundation, American Civil Liberties Union, ACLU of Oregon, the Electronic Privacy Information Center, and the National Association of Criminal Defense Attorneys in Support of Defendant-Appellant and Reversal with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 5,847 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, Times New Roman, size 14 points, using the word processing system Microsoft Word 365.

Dated: May 31, 2024

/s/ Jennifer Stisa Granick
Jennifer Stisa Granick

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate ACMS system on May 31, 2024.

I certify that all participants in the case are registered ACMS users and that service will be accomplished by the appellate ACMS system.

Dated: May 31, 2024

/s/ Jennifer Stisa Granick
Jennifer Stisa Granick

Counsel for Amici Curiae