IN THE SUPREME COURT OF THE STATE OF MONTANA

No. DA 20-0330

STATE OF MONTANA

Plaintiff–Appellee,

v.

BRADLEY MEFFORD,

Defendant–Appellant.

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MONTANA AND AMERICAN CIVIL LIBERTIES UNION FOUNDATION IN SUPPORT OF DEFENDANT–APPELLANT BRADLEY MEFFORD

On Appeal from the Montana Second Judicial District Court,
Silver Bow County, the Honorable Kurt Krueger, Presiding

Brett Max Kaufman
ACLU Foundation
125 Broad Street, 18th Fl.
New York, NY 10004
(212) 549-2500

Alex Rate
Akilah Lane
ACLU of Montana Foundation
P.O. Box 1968
Missoula, MT 59806
(406) 224-1447
ratea@aclumontana.org

Counsel for Amici Curiae

TABLE OF CONTENTS

CERTIFICATE OF SERVICE

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

STATEMENT OF INTEREST OF AMICI

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 of Montana is the local affiliate of the ACLU. The ACLU and the ACLU of Montana have frequently appeared before courts—including this one—throughout the country advocating for Americans' right to privacy based on the Constitutions of both the United States and of Montana, both as direct counsel and as amici curiae. *See e.g.*, *Carpenter v. United States,* 138 S. Ct. 2206 (2018); *People v. Hughes*, 958 N.W.2d 98 (Mich. 2020); *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021); *In re Search Warrant to Google for All Records Associated with Google Account scottarcla@gmail.com*, No. 20CCPC0020 (Cal. Super. Ct., L.A. Cnty. Nov. 12, 2020); *State v. Burch*, 961 N.W.2d 314 (Wisc. 2021); *People v. McCavitt*, No. 125550, 2021 WL 4898748 (Ill. Oct. 21, 2021).

Amici write to address only Issue One raised in the Brief of Appellant, whether the Fourth Amendment and the Montana Constitution prohibit warrantless intrusions into a person's cell phone absent a recognized exception. BoA, filed Oct. 29, 2021, p. 1. In particular, we address the proper scope of searches based on consent, and not whether there was reasonable cause to search Mefford's phone as a probationary search.

INTRODUCTION

Today, virtually everyone carries an electronic device that contains more personal information than could be found in the traditionally most constitutionally protected space—their own homes. *See Riley v. California*, 573 U.S. 373, 395–97 (2014). The more than eighty percent of Americans who own smartphones "keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate." *Id.* at 395. For that reason, the United States Supreme Court, along with other federal courts and state high courts around the country, have over the past decade begun to recognize that more stringent protections against unjustified searches of digital data are necessary to ensure that the public's constitutional rights are not overtaken and undermined by advancing technologies. *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (cell-site location information); *Riley*, 573 U.S. 373 (electronic device search incident to arrest); *United States v. Jones*, 565 U.S. 400 (2012) (warrantless GPS tracking); *People v. Hughes*, 958 N.W.2d 98 (Mich. 2020) (overbroad cell phone searches); *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330 (4th Cir. 2021) (city-wide aerial surveillance).

This case illustrates why exceedingly strong protections against unreasonable searches—including reading the scope of consent-based searches narrowly—are necessary in the digital age. Appellant Mefford's parole officer

asked to view Mefford's phone to confirm Mefford's explanation for why he had committed a technical parole violation—sitting in his apartment complex's parking lot after curfew to obtain Wi-Fi Internet service and talk to his daughter on a messaging app. Mefford agreed to show his text messages with his daughter from that night, and the parole officer reviewed the relevant app data, which confirmed that Mefford was talking to a female person that evening. At that point, the search should have concluded. Instead, the officer exceeded the scope of the consensual search by failing to return Mefford's phone and continuing to look through Mefford's phone to examine Mefford's photo files. The officer did so on his own hunch, and his own say-so. Extending the search beyond the terms of the consent that Mefford gave amounts to unconstrained searching of private digital papers beyond any reasonable interpretation of consent in this case.

When a search is based on consent, that search can go no farther than the consent actually given, even if the officers' purpose in extending the investigation is to look for evidence of the same offense. A consent search is lawful only because the suspect agrees to it. Mefford agreed only to review of his in-app messaging conversation with a specific person on a specific date and time. In order to continue searching beyond the bounds of Mefford's consent, the officer needed to ask for additional consent, get a warrant, or have another exception to the warrant requirement apply.

The Fourth Amendment's purpose is to avoid "giving police officers unbridled discretion to rummage at will among a person's private effects." *Arizona v. Gant*, 556 U.S. 332, 345 (2009); *see also State v. Seader*, 1999 MT 290, ¶¶ 11, 14, 297 Mont. 60, ¶¶ 11, 14, 990 P.2d 180, ¶¶ 11, 14 (discussing Mont. Const. art II, § 11). Narrow permission or justification to search for specific information on an individual's cell phone does not authorize the State to search through *any other* information on the phone. Contrary logic would open the door to just such "general, exploratory rummaging" as the "'general warrant' abhorred by the colonists." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). Consent must be read very narrowly, or the State will be permitted to rummage at will among a person's most personal and private information on the thinnest of justifications. This Court should reject that position.

Moreover, broadening the scope of an individual's consent beyond the bounds of the permission the person expressed and would have reasonably understood to have given opens the door to expansive law enforcement access, copying and storage of an individual's most private information. This expansion would be based solely on an officer's assertion that the subsequent searches and seizures were justified because he wanted to investigate further. As such, it has the potential to eviscerate constitutional protections for privacy and against

unreasonable searches that have heretofore been narrowly and delicately circumscribed.

This Court should ensure that law enforcement is not able to invade Montanans' most private domains without strictly satisfying an exception to the warrant requirement, and it should make clear that the scope of consent to search a cell phone is limited to what a reasonable person would believe from the totality of the circumstances, and nothing more.

ARGUMENT

I. CELL PHONES GENERATE, STORE, AND PROVIDE ACCESS TO VAST QUANTITIES OF SENSITIVE PERSONAL INFORMATION THAT REQUIRE HEIGHTENED CONSTITUTIONAL PROTECTIONS AGAINST WARRANTLESS SEARCHES, ANALYSIS, AND STORAGE.

Modern cell phones contain a wealth of sensitive information that would never have been accessible to law enforcement before the digital age. And today, government agencies have advanced forensic tools that can extract and analyze all of the data stored on a cell phone, including data that the user might not even know exists. When law enforcement searches and analyzes an individual's cell phone data, it invades that individual's expectation of privacy protected by the U.S. and Montana Constitutions, and it must obtain a warrant—or an exception to the warrant requirement, narrowly circumscribed to avoid unmerited intrusion into the vast amounts of personal information now stored on digital devices, must apply.

A. Cell phone searches raise significant privacy concerns because they provide access to vast amounts of personal information.

A smartphone is a palm-sized portal into an individual's personal life, as smartphones "place vast quantities of personal information literally in the hands of individuals." *Riley*, 573 U.S. at 386. In *Riley*, the U.S. Supreme Court recognized that cell phone searches "implicate privacy concerns far beyond those implicated" by the search of any other object and thus require heightened constitutional protections. *Id.* at 393. This is partly because cell phones have become "such a

pervasive and insistent part of daily life"—so much so that they appear almost "an important feature of human anatomy." *Id.* at 385; *see also* Alan Butler, *Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights After* Riley v. California, 10 Duke J. Const. L. & Pub. Pol'y 83, 89–91 (2014).

Cell phone searches involve a quantitatively different privacy intrusion than do searches of physical items because of cell phones' "immense storage capacity." *Riley*, 573 U.S. at 393. And that disparity is only getting more dramatic. In 2014, when the U.S. Supreme Court decided *Riley*, the top-selling smartphone could store sixteen gigabytes of data. *Id.* at 394.[1] The minimum storage on Apple's current line of iPhones is 128 gigabytes and up to one terabyte, equal to roughly twenty continuous days of high definition video, 250,000 personal photos, or six million pages of documents spanning 1,300 physical filing cabinets.[2] Off-device cloud storage services expand capacity even further.[3] Storage capacities increase

[1] Sixteen gigabytes equals about 3,686 songs, 8,672 digital copies of *War and Peace*, 9,830 digital photos, or ten feature-length movies. *See* iClick, *How Big Is a Gig?*, https://perma.cc/32XX-B3QP.

[2] Apple, *Compare iPhone Models*, https://perma.cc/LH9K-BEGC (last visited Jan. 18, 2022). Assoc. Press, *Your Next iPhone Could Have 1 Terabyte of Storage*, NPR (Sept. 14, 2021), https://perma.cc/FZZ6-EGKQ; Dropbox, *How Much is 1 TB of Storage?*, https://perma.cc/SM5K-CUWU (last visited Jan. 18, 2022).

[3] Apple, *iCloud*, https://perma.cc/5UMQ-NV3K (last visited Jan. 18, 2022) (providing up to 2TB of remote storage).

every year, as does the sheer volume of personal data stored on—and accessible from—cell phones.

Cell phones are also qualitatively different from other objects because they "collect[] 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." *Riley*, 573 U.S. at 394. Along with more traditional data like text messages, phone calls, and emails, the proliferation of smartphone apps[4] for social media, health and activity, dating, video streaming, mobile shopping, banking, and password storage have created novel types of records that can "reveal an individual's private interests or concerns." *Id.* at 395. Location information in particular is "detailed, encyclopedic, and effortlessly compiled" by apps whenever a "cell phone faithfully follows its owner . . . into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Carpenter*, 138 S. Ct. at 2216, 2218.

B. Law enforcement is easily and cheaply able to extract, analyze, and store the entire contents of cell phones using advanced forensic tools, especially exacerbating privacy harms from warrantless, unjustified searches.

While this case involved a manual search of a cell phone into areas outside

[4] *See* App Annie, *The State of Mobile 2021* (2021), https://www.appannie.com/en/go/state-of-mobile-2021 (gathering the most popular apps of 2020).

the bounds of the legitimate object of the search, the district court opinion's expansive interpretation of consent could have profound implications given modern advances in law enforcement surveillance technologies. In recent years, law enforcement agencies across the country have acquired powerful new tools to conduct detailed forensic searches of cell phones. These forensic search techniques are problematic because of how much additional personal information the searches can reveal when *all* of the data from a phone is extracted, organized, and categorized in unexpected ways, stored indefinitely, and available to generate leads in cases completely unrelated to the original search.

As discussed above, a police officer's manual search of areas of a phone beyond an individual's limited consent can reveal a great deal of private information. Perusing a person's map data can reveal where and when somebody went to their place of worship, or whether they attended a recent political protest. Clicks on some photographs, a financial app, or a message thread can reveal private medical data. And a scroll through a person's email inboxes, or even a contacts list, can expose a person's other private associations, preferences, or the like.

With technology, access to and analysis of this sensitive information becomes even easier—and even more frightening for privacy. Mobile device forensic tools ("MDFTs") enable law enforcement to first extract and then analyze

a complete copy of a cellphone's contents. Logan Koepke et al., Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 1–2 (Oct. 2020) [hereinafter Upturn Report], https://perma.cc/7DCK-PGMQ.[5] MDFTs extract "the maximum amount of information possible" from a phone, including a user's contacts, call logs, text conversations, photos, videos, saved passwords, GPS location records, phone usage records, online account information, and app data. *Id.* at 10, 16. MDFTs can access data stored remotely in the cloud and even data (like messages and photos) that the user previously deleted. *Id.* at 16–17, 21–23. MDFTs can also use login credentials stored on a phone to extract data from apps and services that are otherwise password-protected. *Id.* at 17–20.

MDFTs enable law enforcement to organize and draw connections in extracted data. They can aggregate data from different apps and sort it by GPS location, file type, or the time and date of creation, enabling police to view the data in ways a phone user cannot and to gain insights that would be impossible if the data were siloed by application. *Id.* at 12. Police can use a MDFT's data-sorting capability to make sense of reams of data and tell a particular story about a person,

[5] Upturn is a 501(c)(3) organization that works in partnership with many of the nation's leading civil rights and public interest organizations to promote equity and justice in the design, governance, and use of digital technology.

including by revealing where they were (and what they were doing), when, with whom, and even why.

Today, law enforcement agencies of all sizes in all fifty states and the District of Columbia have access to these powerful data extraction and analysis tools and use them frequently, placing "[e]very American [] at risk of having their phone forensically searched by law enforcement." *Id.* at 32. At least 2,000 law enforcement agencies nationwide, including in Montana, have purchased MDFTs, while agencies without their own MDFTs often access them through partnerships with MDFT-equipped departments or through federal forensic laboratories. *Id.* at 32, 35, 39; Montana DOJ Attorney General, *Experts Use Digital Forensics to Crack Down on Cyber Crime* (Feb. 25, 2014), https://perma.cc/85UN-3JN7. Many police departments readily admit that they consider MDFTs a standard investigatory tool and use them daily. Upturn Report at 47. At least 50,000 cell phone extractions took place between 2015 and 2019 among the forty-four agencies that reported statistics to Upturn. *Id.* at 41. This is a "*severe undercount*" of the national number, as the vast majority of the agencies that currently use MDFTs did not respond to Upturn's inquiries or did not track MDFT use statistics at all or for the full period covered in the report. *Id.*

Despite the outcome of *Riley*, 573 U.S. at 386, many MDFT searches occur without warrants. Upturn's recent report shows that police frequently conduct

detailed, warrantless forensic searches of cell phone data based on users' purported consent. *Id.* at 46–47.[6] Some examples are striking: of the 1,583 cell phones on which the Harris County, Texas Sheriff's Office performed extractive searches from August 2015 to July 2019, 53 percent were consent searches or searches of "abandoned/deceased" phones. *Id.* at 46. Of the 497 cell phone extractions performed in Anoka County, Minnesota between 2017 to May 2019, 38 percent were consent searches. *Id.* at 47.

Once law enforcement extracts cell phone data, it has the technological capability to store the data forever and search it at will. In this way, through simple consent, the State could come to possess massive amounts of information about a person that, unless subject to legal limitations, could be retained indefinitely and searched at a later date. This is a patently unreasonable power for police to wield—and this Court should make clear that the U.S. and Montana Constitutions do not permit such abuse.

[6] Consent has become an increasingly common justification for searches of physical evidence as well. *See, e.g.*, Ric Simmons, *Not "Voluntary" But Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine*, 80 Ind. L. J. 773 (2005) (more than 90 percent of warrantless searches are accomplished through the use of consent).

II. CONSENT-BASED SEARCHES OF DIGITAL DATA MUST BE NARROWLY SCOPED TO THE OWNER'S EXPLICIT PERMISSION.

Warrantless searches are "per se unreasonable under the Fourth Amendment" unless they fall within one of the "few specifically established and well-delineated exceptions" to the warrant requirement. *Gant*, 556 U.S. at 338 (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)); *State v. Stone*, 2004 MT 151, ¶ 18, 321 Mont. 489, ¶ 18, 92 P.3d 1178, ¶ 18 (discussing Mont. Const. art II, § 11). Once an exception to the warrant requirement is invoked, courts must ensure that its application is "limited in scope to that which is justified by the particular purposes served by the exception." *Florida v. Royer*, 460 U.S. 491, 500 (1983); *accord Collins v. Virginia*, 138 S. Ct. 1663, 1671–72 (2018) (a warrantless search must not be "untether[ed] . . . from the justifications underlying it" (cleaned up)). In the context of searches of electronic devices, the "vast quantities of personal information" at stake make it all the more critical to ask whether application of the exception "to this particular category of effects would 'untether the rule from the justifications underlying the . . . exception.'" *Riley*, 573 U.S. at 386 (quoting *Gant*, 556 U.S. at 343).

A. The search in this case exceeded the scope of Mefford's consent.

Here, the record shows that Mefford gave consent only to a limited search of a single message thread in a specific app, to corroborate that at the time of

Mefford's curfew violation, he was in the parking lot chatting with his daughter. Order at 2; *see* 1/7/19 Tr. at 11; D.C. Doc. 36 at 2. Miller "saw messages between Mefford and his daughter during the hours of concern." Order at 2; *see* 1/7/19 Tr. at 11; D.C. Doc. 36 at 2. But Miller went further, developing his own, unannounced rationale to search through Mefford's photos app. Order at 2; *see* 1/7/19 Tr. at 11; D.C. Doc. 36 at 2.[7] A reasonable person would have understood Mefford's consent to mean that he was granting Miller permission to search his phone so that he could "show him the messages from the time and date that was of concern." 1/7/19 Tr. at 21. It was only after this that Miller took matters into his own hands.

Like warrant-based searches, consent searches are "limited by the terms of [their] authorization." *Walter v. United States*, 447 U.S. 649, 656 (1980). This requirement helps avoid the indiscriminate searches and seizures that were the "immediate evils" motivating adoption of the Fourth Amendment. *Id.* at 657 (citing *Payton v. New York*, 445 U.S. 573, 583 (1980)). It is black letter law that searches and seizures conducted on the basis of consent are reasonable only if conducted within the scope of the consent: "Where items are seized which go beyond the scope of the consent given by a defendant, a successful arrest and prosecution

[7] As Mefford's brief explains, the State never even attempted to introduce evidence supporting Miller's purported justification for expanding his search. App. Br. 7.

based on those items seized cannot pass constitutional muster." *State v. Allies* (1979), 186 Mont. 99, 135, 606 P.2d 1043, 1062 (Shea, J., concurring in part and dissenting in part), *abrogated on other grounds by State v. Cope* (1991), 250 Mont. 387, 819 P.2d 1280. Given that cell phone searches can reveal voluminous amounts of people's most sensitive information, and the enormous privacy implications of allowing broad law enforcement access to this data, courts must narrowly interpret the scope of consent when a cell phone search is in question.

With those principles in mind, and contrary to the district court's reasoning, a reasonable person in Mefford's position would consider their consent to search a cell phone to extend only to categories of data explicitly discussed with law enforcement in lay terms—not a search of other areas of phone. Here, a reasonable person would consider their consent to extend only to the probation officer viewing Mefford's message application to find his conversation with his daughter on the night in question. 1/7/19 Tr. at 23. Mefford did not consent to the officer searching other data on the phone, for that purpose or for any other. 1/7/19 Tr. at 23, 31; App. Br. 8–9, 11–12.

Given the breadth and sensitivity of data on cell phones—the exact kind of information the U.S. Supreme Court said required heightened constitutional protections in *Riley*, 573 U.S. 373—the risks of an overbroad "consent" search to the device owner are severe. And consent searches are especially problematic

because they are conducted without judicial authorization or oversight. Allowing law enforcement to engage in hunch-based searches beyond the reasonably understood bounds of consent would mean that the government could invade any individual's privacy (including victims' and witnesses') without a warrant or other legal justification based only on an officer's mere assertion that his motivation was to search for additional, related evidence.

B. A reasonable person would understand consent to search their cell phone as limited to common-sense categories of relevant information.

As with the search-incident-to-arrest exception analyzed in *Riley*, this Court must assess how to apply a doctrine that originated "in the context of physical objects" such as luggage and vehicles, to this new context involving the "digital content on cell phones" or other electronic devices. 573 U.S. at 386. Consent searches remain permissible in the context of electronic devices, but to avoid narrow grants of consent from enabling sweeping searches of highly sensitive personal data, police and courts must interpret the scope of consent with "scrupulous exactitude." *Cf. Stanford v. Texas*, 379 U.S. 476, 485 (1965). A reasonable person would not believe that giving consent to search a texting app on their cell phone would mean they were giving the police permission to perform a search of photos on the phone (or, even less, to use MDFTs to extract and store all of the phone's data). *See State v. Bailey*, 2010 ME 15, 989 A.2d 716 (a police

officer exceeded the scope of a suspect's consent to search his computer for evidence of another person using his computer without authorization by running a general search of all video files on his computer).

Consent searches have always been limited by the scope of the permission granted. *Florida v. Jimeno*, 500 U.S. 248, 252 (1991); *see United States v. Blocker*, 104 F.3d 720, 728 (5th Cir. 1997) (Inspections are "limited to the purposes contemplated by the [consenting] suspect." (alteration in original) (quoting *United States v. Bosse*, 898 F.2d 113, 115 (9th Cir. 1990))). Especially given the unique nature of digital data and the powerful tools law enforcement agencies now possess, it is objectively reasonable to define consent to search a cell phone as including only a limited, manual search of data relevant to the immediate matter, at least in the absence of clear and unambiguous evidence to the contrary. Otherwise, voluminous and intimate data could be readily subject to indiscriminate police review. The consent exception, which was largely developed prior to the advent of phones that store enormous amounts of data, should not be used to expand access to digital data, which the U.S. Supreme Court has held should be subject to more, not less, Fourth Amendment protection. *Riley*, 573 U.S. at 393.[8]

---

[8] Moreover, "the range of warrantless searches which may be conducted pursuant to Montana's Constitution is narrower than the corresponding range of searches which may be lawfully conducted under the Fourth Amendment to the U.S. Constitution." *State v. Thomas*, 2020 MT 222, ¶ 13, 401 Mont. 175, ¶ 13, 471 P.3d 733, ¶ 13 (citing *State v. Goetz*, 2008 MT 296, ¶ 14, 345 Mont. 421, ¶ 14, 191 P.3d

With that in mind, common knowledge about how cell phones work would limit consensual access to particular categories of data found on a device. When a person looks for information on their own cell phone, they commonly open a particular app, such as text messages or email. They then search that specific category of data, either by scrolling through messages or by typing a query term in the search bar and pressing "Enter." The owner reasonably expects the same common-sense "search" when giving consent to police.

Under the circumstances of this case, the layperson's common-sense understanding that consent applies to particular categories of data on a device, and not to all information, should control. The U.S. Supreme Court's decision in *Riley* rested in part on the observation that "a cell phone's capacity allows even just one type of information to convey far more than previously possible." 573 U.S. at 394. As a result, distinct types of information, usually stored in different parts of a phone, should be analyzed separately. *United States v. Chandler*, No. 20-20476, 2021 WL 5233289, *4–5 (E.D. Mich. November 10, 2021). Just as "[c]onsent to search a garage would not implicitly authorize a search of an adjoining house," *Walter*, 447 U.S. at 656–57, consent to search text messages from last Tuesday

---

489, ¶ 14). And the State bears the burden to establish an exception to the warrant requirement. *Goetz*, ¶ 40.

would not implicitly authorize a search of text messages from last month, let alone photos or a contact list.

This limitation on the categories of data that can be searched would also apply to deleted information, information stored in the cloud, and data, such as incoming messages, that did not exist when law enforcement first received consent to search. Individuals generally do not give consent to a search for information they did not know or expect to be on the phone. For one, accessing data stored on the cloud and not actually resident on the device dramatically expands the scope of a search. *Riley*, 573 U.S. at 397. As the *Riley* Court explained, "[t]reating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. . . . But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen." *Id.* (citations omitted). Further, an ordinary person does not know that data they delete from their device is still "on" it and does not expect that anyone in possession of the phone can access deleted information. *See* Upturn Report at 21–22. When a person deletes data from their phone, they clearly indicate that they do not want anyone, including law enforcement, to look at the data, thus excluding it from the scope of consent. Finally, information like incoming text messages or emails that is received while the phone is in law enforcement's possession cannot be considered within the scope of the original consent.

C. Limitations on consent are particularly important because consent searches of cell phones raise unique concerns about law enforcement coercion.

People may feel coerced to offer consent when law enforcement seizes or threatens to search their cell phones. Scholars and practitioners have long criticized the consent exception to the Fourth Amendment's warrant requirement on policy grounds, often referencing the inherently coercive nature of law enforcement "requests." *See, e.g.*, Marcy Strauss, *Reconstructing Consent*, 92 J. Crim. L. & Criminology 211, 236 (2002) ("most people would not feel free to deny a request by a police officer"); Janice Nadler, *No Need to Shout: Bus Sweeps and the Psychology of Coercion*, 2002 Sup. Ct. Rev. 153, 156 (2002) ("the fiction of consent in Fourth Amendment jurisprudence has led to suspicionless searches of many thousands of innocent citizens who 'consent' to searches under coercive circumstances"). Many have also observed that coercion is particularly present for people of color, and especially Black Americans, who may fear physical harm if they decline a request from a law enforcement officer. *See, e.g.*, Devon W. Carbado, *(E)Racing the Fourth Amendment*, 100 Mich. L. Rev. 946, 971–73, 972 n.121 (2002); *United States v. Washington*, 490 F.3d 765, 768–69, 773 (9th Cir. 2007) (finding recent incidents of white police officers shooting African Americans during traffic stops pertinent to assessment of voluntariness of consent).

In the cell phone context, people may feel additional coercion to consent to a

search just to get their device back. Cell phones perform many essential functions, serving as prescription drug reminders,[9] and lifelines to app-based services such as Uber and Lyft. People who find themselves questioned by law enforcement may feel pressured to acquiesce to search requests to quickly regain access to the device, for example to call the babysitter and say that they've been delayed and will be home late. The inherent coerciveness of consent requests makes it all the more important that the scope of consent be narrowly construed.

CONCLUSION

For these reasons this Court should hold that Mefford's consent to allow the probation officer to see his text messages from the evening in question did not extend to photos on his phone and that the evidence discovered there was obtained unconstitutionally.

[9] J.D. Biersdorfer, *Getting Alerts from a Digital Pill Box*, N.Y. Times (June 5, 2017), https://perma.cc/M4DR-DABR. ("The App Store stocks several pharmaceutical apps designed to organize your pills, schedule doses and remind you to take your medicine.").

DATED this 19th day of January 2022

Brett Max Kaufman
ACLU Foundation
125 Broad Street, 18th Fl.
New York, NY 10004
(212) 549-2500

Alex Rate
Akilah Lane
ACLU of Montana Foundation
P.O. Box 1968
Missoula, MT 59806
(406) 224-1447
ratea@aclumontana.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 11 of the Montana Rules of Appellate Procedure, I certify that this brief is printed with a proportionately-spaced, 14-point Times New Roman typeface; is double spaced (excluding footnotes, quoted, and indented material); has margins of 1-inch; and has a word count of 4,797 words, excluding the exempted Table of Contents, Table of Authorities, Certificate of Compliance, and Certificate of Service.

DATED this 19th day of January 2022

/s/ Alex Rate

Alex Rate
ACLU of Montana Foundation
P.O. Box 1968
Missoula, MT 59806
(406) 224-1447
ratea@aclumontana.org

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on the 19th day of January 2022, I served true and accurate copies of the foregoing Brief of Amici Curiae ACLU Foundation of Montana and ACLU Foundation on the following individuals:

Chad Wright (Counsel for Defendant–Appellant)
Office of State Public Defender
Appellate Defender Division
P.O. Box 200147
Service Method: eService

Eileen Joyce (Counsel for Plaintiff–Appellee)
155 W. Granite Street
Butte, MT 59701
Service Method: eService

Austin Miles Knudsen (Counsel for Plaintiff–Appellee)
215 N. Sanders
Helena, MT 59620
Service Method: eService

Electronically signed by Krystel Pickens on behalf of Alex Rate
DATED this 19th day of January 2022

CERTIFICATE OF SERVICE

I, Alexander H. Rate, hereby certify that I have served true and accurate copies of the foregoing Brief - Amicus to the following on 01-19-2022:

Eileen Joyce (Attorney)
155 W. Granite Street
Butte MT 59701
Representing: State of Montana
Service Method: eService

Austin Miles Knudsen (Govt Attorney)
215 N. Sanders
Helena MT 59620
Representing: State of Montana
Service Method: eService

Kristen Lorraine Peterson (Attorney)
Office of the Appellate Defender
555 Fuller Avenue
Helena MT 59620
Representing: Bradley Mefford
Service Method: eService

Jonathan Mark Krauss (Govt Attorney)
215 N. Sanders
P.O. Box 201401
Helena MT 59620
Representing: State of Montana
Service Method: eService

Electronically signed by Krystel Pickens on behalf of Alexander H. Rate
Dated: 01-19-2022