

IN THE SUPREME COURT OF THE STATE OF MONTANA

No. DA 23-0409

STATE OF MONTANA,

Plaintiff and Appellee,

v.

KATHERINE ANNE PROCTOR,

Defendant and Appellant.

**BRIEF OF *AMICI CURIAE* THE AMERICAN CIVIL LIBERTIES UNION
AND THE ACLU OF MONTANA**

On Appeal from the Montana First Judicial District Court,
Lewis and Clark County, the Honorable Kathy Seeley, Presiding

APPEARANCES:

Alex Rate
ACLU of Montana Foundation, Inc.
P.O. Box 1968
Missoula, MT 59806
(406) 443-8590
ratea@aclumontana.org

Attorney for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

STATEMENT OF INTEREST OF *AMICI CURIAE* 1

SUMMARY OF ARGUMENT 2

ARGUMENT 3

I. The Fourth Amendment and the Montana Constitution Require Stringent Application of the Particularity and Probable Cause Requirements to Prevent Overbroad Warrants for Digital Searches. 3

 A. The Fourth Amendment constrains digital searches by prohibiting general warrants and excessive law enforcement discretion. 4

 B. The Montana Constitution’s heightened privacy analysis builds upon the federal floor and calls for enforcement of particularity and probable cause in the digital search context. 8

II. The Warrant Application in this Case Failed Both the Particularity and the Probable Cause Requirements. 11

 A. The warrant was not particularized because it authorized an overly expansive list of items to search and lacked sufficient temporal limitation. 12

 B. The warrant did not establish probable cause to search all of Defendant’s cell-phone data. 16

III. Sensitive Factual Circumstances Like These Demand that Courts Diligently Enforce Constitutional Privacy Protections. 18

CONCLUSION 21

CERTIFICATE OF COMPLIANCE 23

CERTIFICATE OF SERVICE 24

TABLE OF AUTHORITIES

CASES

| | |
|--|-------------|
| <i>Arizona v. Gant</i> , 556 U.S. 332 (2009)..... | 2, 5 |
| <i>Berger v. New York</i> , 388 U.S. 41 (1967)..... | 4 |
| <i>Boyd v. United States</i> , 116 U.S. 616 (1886)..... | 4 |
| <i>Buckham v. State</i> , 185 A.3d 1 (Del. 2018)..... | 17 |
| <i>Burns v. United States</i> , 235 A.3d 758 (D.C. 2020)..... | 12 |
| <i>Carpenter v. United States</i> , 585 U.S. 296 (2018)..... | 1, 6, 7, 15 |
| <i>Hauge v. District Court</i> , 2001 MT 255, 307 Mont. 195, 36 P.3d 947..... | 13 |
| <i>Horton v. California</i> , 496 U.S. 128 (1990)..... | 6 |
| <i>Kyllo v. United States</i> , 533 U.S. 27 (2001)..... | 4 |
| <i>Maryland v. Garrison</i> , 480 U.S. 78 (1987)..... | 4, 14 |
| <i>People v. Coke</i> , 461 P.3d 508 (Colo. 2020)..... | 16 |
| <i>People v. Hughes</i> , 958 N.W.2d 98 (Mich. 2020)..... | 7 |

| | |
|--|--------------------|
| <i>People v. Thompson</i> , 178 A.D.3d 457 (N.Y. App. Div. 2020)..... | 15 |
| <i>Riley v. California</i> , 573 U.S. 373 (2014)..... | 2, 6, 7, 8, 11, 17 |
| <i>Stanford v. Texas</i> , 379 U.S. 476 (1965)..... | 4 |
| <i>State v. Allen</i> , 2010 MT 214, 357 Mont. 495, 241 P.3d 1045..... | 8 |
| <i>State v. Bar-Jonah</i> , 2004 MT 344, 324 Mont. 278, 102 P.3d 1229..... | 10 |
| <i>State v. Graham</i> , 2004 MT 385, 325 Mont. 110, 103 P.3d 1073..... | 14 |
| <i>State v. Hardaway</i> , 2001 MT 252, 307 Mont. 139, 36 P.3d 900..... | 2 |
| <i>State v. Henderson</i> , 854 N.W.2d 616 (Neb. 2014)..... | 12 |
| <i>State v. Mansor</i> , 421 P.3d 323 (Or. 2018)..... | 15 |
| <i>State v. McLawhorn</i> , 636 S.W.3d 210 (Tenn. Crim. App. 2020)..... | 16 |
| <i>State v. Mefford</i> , 2022 MT 185, 410 Mont. 146, 517 P.3d 210..... | 1, 9, 10, 11 |
| <i>State v. Missak</i> , 299 A.3d 821 (N.J. Super. Ct. App. Div. 2023)..... | 15 |
| <i>State v. Peoples</i> , 2022 MT 4, 407 Mont. 84, 502 P.3d 129..... | 10 |
| <i>State v. Seader</i> , 1999 MT 290, 297 Mont. 60, 990 P.2d 180..... | 9, 10, 13 |

| | |
|--|------|
| <i>State v. Staker</i> , 2021 MT 151, 404 Mont. 307, 489 P.3d 489..... | 8 |
| <i>State v. Urziceanu</i> , 2015 MT 58, 378 Mont. 313, 344 P.3d 399..... | 8 |
| <i>State v. Wilson</i> , 884 S.E.2d 298 (Ga. 2023)..... | 13 |
| <i>Taylor v. State</i> , 260 A.3d 602 (Del. 2021)..... | 14 |
| <i>Terreros v. State</i> , 312 A.3d 651 (Del. 2024)..... | 13 |
| <i>United States v. Atencio</i> , 2022 WL 1288734 (D. Idaho Apr. 29, 2022)..... | 12 |
| <i>United States v. Chadwick</i> , 433 U.S. 1 (1977)..... | 6 |
| <i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013)..... | 7 |
| <i>United States v. Grant</i> , 682 F.3d 827 (9th Cir. 2012)..... | 6 |
| <i>United States v. Heckenkamp</i> , 482 F.3d 1142 (9th Cir. 2007)..... | 6 |
| <i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006)..... | 4, 5 |
| <i>United States v. Hillyard</i> , 677 F.2d 1336 (9th Cir. 1982)..... | 5 |
| <i>United States v. Jones</i> , 565 U.S. 400 (2012)..... | 8 |
| <i>United States v. Kow</i> , 58 F.3d 423 (9th Cir. 1995)..... | 5 |

| | |
|---|------|
| <i>United States v. Lauria</i> , 70 F.4th 106 (2d Cir. 2003)..... | 18 |
| <i>United States v. Lofstead</i> , 574 F. Supp.3d 831 (D. Nev. 2021)..... | 15 |
| <i>United States v. Mercery</i> , 591 F.Supp.3d 1369 (M.D. Ga. 2022)..... | 12 |
| <i>United States v. Morton</i> , 984 F.3d 421 (5th Cir. 2021)..... | 16 |
| <i>United States v. Oglesby</i> , 2019 WL 1877228 (S.D. Tex. Apr. 26, 2019)..... | 17 |
| <i>United States v. Otero</i> , 563 F.3d 1127 (10th Cir. 2009)..... | 7 |
| <i>United States v. Ramirez</i> , 180 F.Supp.3d 491 (W.D. Ky. 2016)..... | 18 |
| <i>United States v. Stubbs</i> , 873 F.2d 210 (9th Cir. 1989)..... | 5 |
| <i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010)..... | 6 |
| <i>Warden, Md. Penitentiary v. Hayden</i> , 387 U.S. 294 (1967)..... | 4, 5 |
| CONSTITUTIONAL PROVISIONS | |
| Mont. Const. art. II, § 10..... | 8 |
| Mont. Const. art. II, § 11..... | 8, 9 |
| U.S. Const. amend. IV..... | 2 |
| OTHER AUTHORITIES | |
| 5 Mont. Const. Conv. Tr. (Mar. 7, 1972)..... | 8, 9 |

Am. Bar Ass’n, *Trauma Caused by Separation of Children from Parents: A Tool to Help Lawyers* (Jan. 2020)..... 19

Darrell Ehrlick, *Report finds problems with foster child program, including missing protection and safety plans*, Daily Montanan (Jan. 6, 2022)..... 20

Deana Around Him, *American Indian and Alaska Native (AIAN) Children Are Overrepresented in Foster Care States With the Largest Proportions of AIAN Children*, Child Trends (Nov. 8, 2022)..... 20

Human Rights Watch & ACLU, *“If I Wasn’t Poor, I Wouldn’t Be Unfit”:* *The Family Separation Crisis in the US Child Welfare System* (Nov. 2022)..... 19, 20

Mara Silvers, *Can Montana mend its racial gap in foster care?*, Mont. Free Press (Feb. 14, 2024)..... 20, 21

Tarek Z. Ismail, *Family Policing and the Fourth Amendment*, 111 Cal. L. Rev. 12 1485..... 19

STATEMENT OF INTEREST OF *AMICI CURIAE*

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles embodied in federal and state constitutions and our nation’s civil rights laws. The ACLU of Montana is the local affiliate of the ACLU. Both entities frequently appear before courts, including this one, to advocate for Americans’ right to privacy in the digital context based on the Constitutions of both the United States and of Montana, as direct counsel and as *amicus curiae*.¹ See, e.g., *Carpenter v. United States*, 585 U.S. 296 (2018); *State v. Mefford*, 2022 MT 185, 410 Mont. 146, 517 P.3d 210.

¹ This brief was prepared with the assistance of Suchait Kahlon and Benjamin Lerude, students in the New York University (“NYU”) School of Law Technology Law and Policy Clinic. The clinic operates under Washington Square Legal Services, Inc., a not-for-profit corporation affiliated with the NYU School of Law. The brief does not purport to present the institutional views of NYU School of Law.

SUMMARY OF ARGUMENT

The Fourth Amendment prohibits general warrants that “giv[e] police officers unbridled discretion to rummage at will among a person’s private effects.” *Arizona v. Gant*, 556 U.S. 332, 345 (2009). It does so by requiring warrants to be supported by probable cause and particularized to the places and things to be searched and seized. U.S. Const. amend. IV. Above this federal floor, “Montana’s unique constitutional language affords citizens a greater right to privacy, and therefore, broader protection than the Fourth Amendment in cases involving searches” *State v. Hardaway*, 2001 MT 252, ¶ 31, 307 Mont. 139, 36 P.3d 900. In a matter of first impression, this case requires this Court to apply Montana’s privacy-enhanced standard and enforce the particularity and probable cause requirements in the digital search context. Establishing clear protections against overbroad warrants for digital searches and seizures will prevent police from gaining unconstitutional access to “digital record[s] of nearly every aspect of [Montanans’] lives.” *Riley v. California*, 573 U.S. 373, 395 (2014).

To satisfy the particularity and probable cause requirements, respectively, warrant applications for digital searches must articulate (1) the specific data being sought, and (2) the nexus between that data and the probable cause supporting the warrant. Just as probable cause to search specific spaces cannot authorize the search of an entire home, warrants for digital searches cannot authorize the search

of *all* data on a device—every application, message, photo, location, and more. Warrant applications must include limiting factors—for example, narrowing searches to relevant time windows—to ensure that officers cannot exercise unlimited discretion when conducting searches.

Here, the warrant was unconstitutional under both the federal and Montana constitutions because it satisfied neither the particularity nor the probable cause nexus requirement. It authorized an over-inclusive list of data to be searched, lacked temporal limitations, and failed to establish a probable cause nexus, permitting police to search all of Defendant’s cell-phone data spanning several months. The sensitive factual circumstances of family investigations like the one in this case demand that this Court diligently uphold Montanans’ fundamental privacy rights.

ARGUMENT

I. The Fourth Amendment and the Montana Constitution Require Stringent Application of the Particularity and Probable Cause Requirements to Prevent Overbroad Warrants for Digital Searches.

Both the federal and Montana constitutions require that warrant applications for digital searches satisfy the particularity and probable cause requirements. Under these standards, this Court should suppress the evidence obtained from the warrant in this case. In doing so, it should provide needed guidance for lower courts and law enforcement to protect Montanans’ digital privacy going forward.

A. The Fourth Amendment constrains digital searches by prohibiting general warrants and excessive law enforcement discretion.

The Framers intended the Fourth Amendment to prohibit general warrants, which were employed by the British Crown as “instruments of oppression.” *Stanford v. Texas*, 379 U.S. 476, 482 (1965). The unbridled discretion given to British officials infuriated American colonists, who denounced general warrants as “the worst instrument[s] of arbitrary power” because they placed “the liberty of every man in the hands of every petty officer.” *Boyd v. United States*, 116 U.S. 616, 625 (1886) (citation omitted). Underlying the Fourth Amendment, therefore, is a special concern for “the sanctity of a man’s home and the privacies of life.” *Id.* at 630; *see also Kyllo v. United States*, 533 U.S. 27, 40 (2001).

Because of this disdain for general warrants, the Fourth Amendment prohibits “all ‘unreasonable’ searches and seizures” and “require[s] the use of warrants, which particularly describe ‘the places to be searched, and the persons or things to be seized.’” *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 301 (1967) (citation omitted). The “manifest purpose” of the particularity requirement was to prevent general searches. *Maryland v. Garrison*, 480 U.S. 78, 84 (1987); *see also Berger v. New York*, 388 U.S. 41, 58 (1967) (the particularity requirement “makes general searches . . . impossible” (citation omitted)).

A warrant is sufficiently particular when it “clearly states what is sought” and “imposes a meaningful restriction upon the objects to be seized.” *United States*

v. Hill, 459 F.3d 966, 973 (9th Cir. 2006) (citation omitted). This means that a warrant is unlawfully general when it “le[aves] to the executing officers,” rather than to the issuing magistrate, “the task of determining what items f[a]ll within broad categories stated in the warrant.” *United States v. Hillyard*, 677 F.2d 1336, 1339 (9th Cir. 1982) (citation omitted). Warrants must clearly distinguish between property that is and is not subject to search. For example, the Ninth Circuit has held that a warrant without limiting descriptions—such as the names of companies involved in an illegal scheme—was insufficiently particular, *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995), and that police could not seize all of a defendant’s office documents when a warrant lacked specific descriptions of those documents, *United States v. Stubbs*, 873 F.2d 210, 211 (9th Cir. 1989).

The particularity analysis is interconnected with another essential mandate of the Fourth Amendment: a warrant must be supported by probable cause. The probable cause requirement protects people in two ways: it ensures adequate justification for a search or seizure, *see Gant*, 556 U.S. at 345, and limits its scope, *see Hill*, 459 F.3d at 973.

Together, the particularity and probable cause requirements ensure not only that officers have a proper basis to conduct a search, but also that searches are limited to places and things directly tied to that basis. *See Hayden*, 387 U.S. at 307 (there must “be a nexus . . . between the item to be seized and criminal behavior”).

The “nexus” requirement means that an officer may not open a small medicine cabinet when a warrant authorizes a search for a rifle in someone’s home, *Horton v. California*, 496 U.S. 128, 141 (1990), or search a suspect’s house merely because at one point they possessed a weapon thought to have been used in a crime outside the home, *United States v. Grant*, 682 F.3d 827, 832–33 (9th Cir. 2012).

With the Fourth Amendment, the Framers were not merely “focused on the wrongs of that day.” *United States v. Chadwick*, 433 U.S. 1, 9 (1977). Instead, they recognized the need “to safeguard fundamental values which would far outlast the specific abuses which gave it birth.” *Id.* The U.S. Supreme Court has agreed that the Fourth Amendment must adapt to modern contexts to preserve the appropriate balance between privacy and the law enforcement interests that existed at our country’s founding. *See Riley*, 573 U.S. at 386; *Carpenter*, 585 U.S. at 311.

As digital technologies have become ever more pervasive, courts have applied stringent protections against unfettered police access in a variety of digital contexts. *See, e.g., Carpenter*, 585 U.S. at 309–12 (cell-site location information); *Riley*, 573 U.S. at 395–96 (search and browsing history); *United States v. Heckenkamp*, 482 F.3d 1142, 1145 (9th Cir. 2007) (password-protected computer files); *United States v. Warshak*, 631 F.3d 266, 274 (6th Cir. 2010) (e-mail).

The particularity requirement has “heightened sensitivity . . . in the context of digital searches” because of the vast amounts of personal information accessible

through our devices. *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013); *see also, e.g., United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (computers’ ability to store “a huge array” of information “makes the particularity requirement that much more important”). The U.S. Supreme Court has repeatedly emphasized this point. For example, in *Riley*, 573 U.S. at 394, it explained that digital devices the size of a human palm can store practically unlimited quantities of data, and in *Carpenter*, 585 U.S. at 298, it expressed concern that police conducting digital searches might overstep the bounds of their permitted search with just a few taps and clicks. State courts have mirrored these concerns. For example, the Michigan Supreme Court held that police were not permitted to search for evidence of a crime not identified in the warrant because doing so would “effectively nullify the particularity requirement . . . in the context of cell-phone data.” *People v. Hughes*, 958 N.W.2d 98, 117 (Mich. 2020).

Not only is the quantity of data stored on our devices greater than in analog contexts, the data on our devices is also qualitatively different from evidence ordinarily accessible in our non-digital “persons, houses, papers, and effects.” Because digital devices “collect[] in one place many distinct types of information”—addresses, notes, prescriptions, bank statements, videos, etc.—digital data “reveal much more in combination than any isolated record,” and much more about “an individual’s private interests or concerns.” *Riley*, 573 U.S. at 394–

95. For example, location data expose not only a person’s movements but also “a wealth of detail about her familial, political, professional, religious, and sexual associations.” *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

B. The Montana Constitution’s heightened privacy analysis builds upon the federal floor and calls for enforcement of particularity and probable cause in the digital search context.

The Montana Constitution was drafted with the intent “to provide greater protection to individual rights than does the Fourth Amendment.” *State v. Urziceanu*, 2015 MT 58, ¶ 11, 378 Mont. 313, 344 P.3d 399; *see also* 5 Mont. Const. Conv. Tr. 1680 (Mar. 7, 1972) (quoting Bill of Rights Committee delegate Bob Campbell as asserting that “the times have changed sufficiently that [privacy rights] should now be recognized” in the Montana Constitution). To this end, Montana’s constitutional delegates adopted *both* a search and seizure provision nearly identical to the Fourth Amendment *and* a provision expressly recognizing Montanans’ individual right to privacy. Mont. Const. art. II, §§ 10–11. Together, these two provisions “provide a heightened state right to privacy, broader where applicable than the [federal] privacy protection.” *State v. Staker*, 2021 MT 151, ¶ 9, 404 Mont. 307, 489 P.3d 489.

Montana’s privacy provision was “intended to be dynamic,” “to keep pace with and not be outstripped by technological developments.” *State v. Allen*, 2010

MT 214, ¶ 55, 357 Mont. 495, 241 P.3d 1045. Its sponsors recognized that with the advancements of “an increasingly complex society . . . our area of privacy has decreased, decreased, and decreased.” 5 Mont. Const. Conv. Tr. at 1681 (quoting Delegate Campbell). The delegates constitutionalized the right to privacy out of concern that individual privacy interests would only be further weakened by constantly evolving technologies. *See, e.g., id.* at 1682 (Delegate Campbell testifying that “the people of Montana should be protected as much as possible against eavesdropping, electronic surveillance, and such type of activities”); *id.* at 1687 (Wade Dahood, Chairman of the Bill of Rights Committee, stating that “we cannot conceive of a situation where we could ever permit electronic surveillance”).

Five decades later, in 2022, Montanans furthered the drafters’ vision of technological responsiveness by inserting “electronic data and communications” into the Constitution’s search and seizure provision. Mont. Const. art. II, § 11. Though this type of information was already protected by the provision as one’s “papers . . . and effects,” *see, e.g., Mefford*, 2022 MT 185, ¶ 15, the amendment underscores Montana’s continued commitment to constraining digital-age searches.

This Court has already long enforced the particularity requirement in the physical search context “to prevent a ‘general, exploratory rummaging in a

person’s belongings.” *State v. Seader*, 1999 MT 290, ¶ 11, 297 Mont. 60, 990 P.2d 180 (citation omitted). When evaluating particularity, courts assess whether or not “a more precise description of the items to be seized is [] possible.” *Id.*, ¶ 13. The warrant application “must be specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized,” though it need not be “elaborately detailed.” *State v. Bar-Jonah*, 2004 MT 344, ¶ 64, 324 Mont. 278, 102 P.3d 1229 (citation omitted). The probable cause nexus requirement also factors into Montana’s heightened privacy analysis, as a search is only valid if “the manner of execution” matches the justification for the search. *State v. Peoples*, 2022 MT 4, ¶ 24, 407 Mont. 84, 502 P.3d 129. Though these standards require more diligence from police, this Court rightfully “refuse[s] to compromise Fourth Amendment rights and those guaranteed by Article II, Section 11 of the Montana Constitution for the sake of efficient law enforcement.” *Seader*, 1999 MT 290, ¶ 15.

Against the backdrop of these robust constitutional privacy protections, this Court has begun to make clear that traditional warrant requirements forcefully apply in the digital context. Two years ago, in *Mefford*, the Court recognized the risk that digital searches “expose to the government far *more* than the most exhaustive search of a house: A 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.” 2022 MT 185, ¶ 15 (quoting *Riley*, 573 U.S. at 396–97). To limit police access to this sensitive information, the *Mefford* Court held that authorization to search *certain data* on a cell-phone does *not* permit the search of *all data*. *Id.*, ¶ 29 (“*Mefford*’s consent to search Facebook Messenger for [a] limited purpose . . . did not give [the officer] permission to access *Mefford*’s digital photo gallery on his phone.”). There, the narrow scope of consent limited what the officer could search. Here, this Court must enforce the particularity and probable cause nexus requirements to appropriately limit the scope of digital search warrants and protect Montanans’ digital privacy.

II. The Warrant Application in this Case Failed Both the Particularity and the Probable Cause Requirements.

The Fourth Amendment and the Montana Constitution require that police officers describe not only *what* data they seek to access, but also *how* that specific data is responsive to the probable cause justifying the warrant. In this case, the warrant satisfied neither the particularity nor the probable cause nexus requirements because it granted police unrestrained authority to search all data on Defendant’s cell-phone for an investigation of specific injuries to a child, lacked limiting factors such as specific time frames for the search, and was based on broad, generic justifications that facilitated the unbridled police discretion prohibited by the federal and state constitutions.

A. The warrant was not particularized because it authorized an overly expansive list of items to search and lacked sufficient temporal limitation.

This warrant was a general one. It failed to limit itself to data justified by probable cause. *See, e.g., Burns v. United States*, 235 A.3d 758, 775 (D.C. 2020) (warrant authorizing search for generic categories of data for which there was no probable cause was “constitutionally intolerable”). Instead, it laid out an expansive list of items, including Defendant’s browsing history, location history, private social media content, and practically any means by which one may communicate via or store data on a cell-phone. Courts have invalidated similar warrants permitting police to search essentially an entire cell-phone, *see United States v. Atencio*, 2022 WL 1288734, at *19–20 (D. Idaho Apr. 29, 2022), or virtually all the information in a social media account, *see United States v. Mercery*, 591 F.Supp.3d 1369 (M.D. Ga. 2022).

Additionally, the warrant’s phrase “including but not limited to” granted police unrestrained discretion to search data beyond that enumerated in the warrant. Other courts have held that this kind of phrase fails the particularity requirement because it insufficiently limits potentially vast cell-phone searches. For instance, in *State v. Henderson*, the Nebraska Supreme Court stated that a warrant authorizing the search of “[a]ny and all information” on a cell-phone was not particularized. 854 N.W.2d 616 (Neb. 2014). Last year, the Georgia Supreme

Court suppressed digital data obtained from a warrant containing the exact phrase used here (“including but not limited to”) because it was not sufficiently particularized. *See State v. Wilson*, 884 S.E.2d 298, 300–01 (Ga. 2023).

This Court has already held that catch-all terms are insufficiently particular for physical searches. For example, in *Hauge v. District Court*, this Court severed the phrase “anything else of value” from a warrant authorizing a search for evidence of drug-related activities because it was overbroad. 2001 MT 255, ¶ 19, 307 Mont. 195, 36 P.3d 947. And in *Seader*, the Court found use of the same phrase unconstitutional after an officer admitted that he could not “conceive of anything which wouldn’t be covered by that language.” 1999 MT 290, ¶ 14–15. While there has been no occasion to apply this reasoning to warrants for digital searches, the warrant here requires this Court to affirm that catch-all phrases are unconstitutional in both digital and analog contexts.

Additionally, the warrant’s requirement that data be “related to the crimes or offenses identified herein” was not an adequate limitation. After all, it is impossible to know whether data “related to the crime” will be found in one’s login history, documents, social media, bank accounts, photos, or messages until *after* such data has been accessed by law enforcement. Earlier this year, the Delaware Supreme Court suppressed a warrant that authorized police to broadly search all cell-phone apps “used or intended to be used” to commit the investigated

crime. *Terreros v. State*, 312 A.3d 651, 667 (Del. 2024). Here, police might have had probable cause to search *some* of Defendant’s text messages with her husband, but they lacked the basis to look through virtually *all* of her cell-phone data.

Warrants do not allow police to search anywhere for anything that *during the search* might turn out to be relevant; instead, they only authorize search of specific data when there is probable cause *before the search* to believe evidence of a crime will be found there. Along these lines, more specificity is required than simply identifying the cell-phones to be searched and allowing investigators to search all data pertinent to the investigation. *See Taylor v. State*, 260 A.3d 602, 616 (Del. 2021). Similarly, a warrant to search a house for anything “related to the crimes or offenses identified herein” would impose no meaningful restraint and amount to a general warrant. *Garrison*, 480 U.S. at 84. Any rule that says otherwise will authorize exactly the kind of invasive “fishing expeditions” that are constitutionally prohibited. *Id.*; *see also State v. Graham*, 2004 MT 385, ¶ 25, 325 Mont. 110, 103 P.3d 1073.

In this case, the overbreadth of the warrant’s long, template-like list of data to be searched was exacerbated by the lack of temporal limitation. For a digital search warrant to be sufficiently particularized, it should generally constrain the data to be searched to dates around when the alleged crime occurred. Temporal limitations are especially important for digital warrants because access to extended

periods of data increases the potential for police to obtain sensitive information encompassing “every aspect of people’s lives.” *See Carpenter*, 585 U.S. at 311. For this reason, courts have invalidated warrants when the government “knew exactly when the phone was used to commit the target offense” but failed to “tailor” the search to those specific days. *United States v. Lofstead*, 574 F. Supp.3d 831, 843 (D. Nev. 2021); *see also State v. Missak*, 299 A.3d 821 (N.J. Super. Ct. App. Div. 2023) (a warrant that purported to permit search of all of a cell-phone’s contents for evidence of a crime which allegedly took place over a two-day period was too broad).

This warrant lacked a sufficient temporal limitation. It failed to explicitly provide any limiting time frame and instead permitted searching all data “related to the crimes or offenses identified.” The district court inferred that “related” data could have only existed since the child P.P.’s birth on May 28, 2021—five months before police obtained a warrant. But even if the warrant had included this temporal constraint, neither five months nor an alleged victim’s entire lifetime are appropriately constrained time periods. State courts are unequivocal on this point, ruling that probable cause to investigate a crime which took place over a one-day period does not permit search of over eight months of cell-phone data, *see People v. Thompson*, 178 A.D.3d 457 (N.Y. App. Div. 2020), and that police may not search data from months before a victim’s death, *see State v. Mansor*, 421 P.3d

323, 343–44 (Or. 2018). The police knew the specific dates when P.P. exhibited injuries and could have easily crafted a warrant focused on those time frames. A warrant that “contains no particularity as to . . . the time period during which the [crime] allegedly occurred” must be held overbroad. *See People v. Coke*, 461 P.3d 508, 516 (Colo. 2020).

B. The warrant did not establish probable cause to search all of Defendant’s cell-phone data.

Probable cause was not established to seize all the items described in the warrant. Even assuming that the information detailed in the affidavit—*i.e.*, P.P.’s documented injuries, the officer’s conversations with daycare employees, and the physicians’ diagnoses—was sufficient to establish probable cause that Defendant may have injured her daughter, that probable cause only justified a search of *some* of Defendant’s data. In *United States v. Morton*, the Fifth Circuit considered a warrant that authorized a search for text messages, call logs, contacts, and photographs. Because the warrant did not establish probable cause that relevant evidence would be in photograph form, the photographs were suppressed. 984 F.3d 421 (5th Cir. 2021), *rev’d on other grounds*, 46 F.4th 331 (2022) (en banc). Similarly, the Tennessee Criminal Court of Appeals held that probable cause to determine whether a suspect’s cell-phone had a flashlight function did not authorize general rummaging through the cell-phone. *State v. McLawhorn*, 636 S.W.3d 210, 242–44 (Tenn. Crim. App. 2020).

Officer VanDyke’s warrant application relied on broad assertions based on his “training and experience,” such as that “[c]riminals will often use voicemail messages, text messages, pictures messages, and other wireless communication methods to facilitate their crimes.” 8/26/22 Hr. Ex. 27, Application at 7–8. But such generic assertions do not provide sufficient basis to search virtually all of a defendant’s cell-phone data. Otherwise, “every accusation of criminal activity would automatically authorize a search of the suspect’s cell-phone, transforming every arrest warrant into a search warrant and directly contravening the Supreme Court’s decision in *Riley*.” *United States v. Oglesby*, 2019 WL 1877228, at *6 (S.D. Tex. Apr. 26, 2019). Courts have therefore rejected the notion that a probable cause nexus can be established by an officer’s assertion that criminals frequently use digital devices to commit crimes. As the Delaware Supreme Court stated when rejecting a similar effort by police to justify a broad warrant based on an officer’s training and experience, “[p]articularly unpersuasive was the statement that ‘criminals often communicate through cell phones’”—after all, “who doesn’t in this day and age?” *Buckham v. State*, 185 A.3d 1, 17 (Del. 2018).

The warrant application also noted that “[c]ellular telephones often hold . . . data pertaining to the health and wellbeing of the cell-phone’s owner, their children, and family members,” and that Defendant used her cell-phone soon after learning of her daughter’s diagnosis. 8/26/22 Hr. Ex. 27, Application at 7–8. But

the mere possession of a cell-phone around the time of an alleged crime is similarly insufficient to justify an intrusive search of a phone. At least one federal district court has ruled that possessing a cell-phone during one's arrest cannot by itself establish a nexus between the cell-phone and criminal activity even if co-conspirators usually communicate via cell phone. *See United States v. Ramirez*, 180 F.Supp.3d 491 (W.D. Ky. 2016). And in *United States v. Lauria*, the Second Circuit held that communication between suspects' cell-phone numbers shortly before an alleged robbery was insufficient to establish probable cause to obtain months of location information. 70 F.4th 106, 128–29 (2d Cir. 2003).

III. Sensitive Factual Circumstances Like These Demand that Courts Diligently Enforce Constitutional Privacy Protections.

The high stakes of child abuse allegations should activate courts to be *more* vigilant of procedural shortcuts that jeopardize constitutional rights, not less. Child abuse allegations can involve weighty harms that must be taken seriously. But for the same reason, the stakes for parents suspected of wrongdoing are also immense, especially when allegations are unfounded. Courts must apply constitutional privacy protections at the earliest stages of police involvement to minimize the possibility of unsubstantiated allegations and subsequent harms. This will prevent police from improperly intruding into constitutionally protected spaces, including

digital ones, in emotionally charged contexts. It will also ensure that when investigations bear fruit, the resulting charges are sustainable, lawful, and just.

In this case, police became involved only after P.P. was diagnosed with Shaken Baby Syndrome (“SBS”)—a scientifically unreliable diagnosis²—and after a hospital social worker reported P.P.’s condition to Child Protective Services (“CPS”). CPS investigations and criminal investigations involving families are often intertwined in this way. *See, e.g.,* Tarek Z. Ismail, *Family Policing and the Fourth Amendment*, 111 Cal. L. Rev. 1485, 1501. Investigations based upon allegations of abuse or neglect can trigger a child’s removal from their family at any time “before, during, or after the investigation period.” Human Rights Watch & ACLU, *“If I Wasn’t Poor, I Wouldn’t Be Unfit”: The Family Separation Crisis in the US Child Welfare System* 70 (Nov. 2022). Removal and subsequent placement of a child into the foster care system does not guarantee better outcomes; instead, “[c]hildren who are removed from their homes experience poorer outcomes compared to their peers,” including in mental health, cognitive development, and education. *Id.* at 117; *see also* Am. Bar Ass’n, *Trauma Caused by Separation of Children from Parents: A Tool to Help Lawyers* 6–25 (Jan. 2020). And allegations can have devastating impact even if no wrongdoing is found:

² Though beyond this brief’s scope, *amici* agree with Appellant that because SBS diagnoses are scientifically unreliable, expert testimony offering SBS diagnoses should be held inadmissible.

parents subject to a single unsubstantiated investigation may be placed on a child welfare registry for years to come, which “often results in denial of employment” and other consequences tied to the stigma of being system-involved. *See* Human Rights Watch & ACLU, *supra* at 63–64, 125–27. Even so, a staggering 83% of reports nationwide are unsubstantiated upon investigation. *Id.* at 66.

These harms are not experienced equally. Both nationwide and in Montana, families impacted by child welfare investigations “are disproportionately communities of color, especially Black and Indigenous families, and people living in poverty.” *Id.* at 3. Montana now has one of the highest rates of children in foster care. *See* Darrell Ehrlick, *Report finds problems with foster child program, including missing protection and safety plans*, Daily Montanan (Jan. 6, 2022). Native American children constitute only 9 percent of Montana’s child population, but 36 percent of its foster care population. Deana Around Him, *American Indian and Alaska Native (AIAN) Children Are Overrepresented in Foster Care in States With the Largest Proportions of AIAN Children*, Child Trends (Nov. 8, 2022). Child welfare experts in Montana attribute this 400 percent overrepresentation to “unequal access to economic opportunity and health care resources in Native communities and deeply rooted biases held by child protection authorities about what safe and stable families look like,” rather than any meaningful parenting differences. *See* Mara Silvers, *Can Montana mend its racial gap in foster care?*,

Mont. Free Press (Feb. 14, 2024). The racial inequities of Montana’s child welfare system can only be understood within this nation’s long history of subjecting Native families to disparate enforcement and forced assimilation. *Id.*

These dynamics underscore the importance of rigorously applying procedural safeguards against privacy infringement—like the particularity and probable cause nexus requirements—to digital searches and seizures conducted in the context of child abuse investigations. When a court grants a warrant, it does not merely authorize a single search; it also catalyzes a sequence of events that, when unjustified, can lead to potentially catastrophic outcomes for Montana’s children and families. This is especially true for digital search warrants, for which the risk of over-exposing vast troves of intimate data is exponentially greater. If children are endangered, police should be capable of articulating with particularity *what* evidence they seek and *how* it supports their theory of harm; if they cannot, then a court should not permit the invasion of a family’s privacy or the harms that flow from it. With stakes so high, it is especially critical that this Court enforce the procedural constraints of search and seizure doctrine.

CONCLUSION

The particularity and probable cause requirements of the Fourth Amendment and the Montana Constitution prohibit warrants that authorize the unlimited search of all data on a device, lack temporal limitations, and fail to establish a probable

cause nexus between the data sought and the crime being investigated. This Court must enforce these standards in the digital context and find the warrant in this case unconstitutional.

DATED this 16th day of December 2024

/s/Alex Rate

Alex Rate

ACLU of Montana Foundation

P.O. Box 1968

Missoula, MT 59806

(406) 443-8590

ratea@aclumontana.org

Attorney 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 proportionally-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 4,958 words, including footnotes and excluding the exempted Table of Contents, Table of Authorities, Certificate of Compliance, and Certificate of Service.

DATED this 16th day of December 2024

/s/ Alex Rate

Alex Rate

ACLU of Montana Foundation

P.O. Box 1968

Missoula, MT 59806

(406) 443-8590

ratea@aclumontana.org

Attorney for Amici Curiae

CERTIFICATE OF SERVICE

I, Krystal Pickens, hereby certify that on the 16th day of December 2024, I served true and accurate copies of the foregoing Brief of *Amici Curiae* American Civil Liberties Union and the ACLU of Montana to the following individuals:

Alexander H. Pyle
Office of the Appellate Defender
555 Fuller Avenue
Helena, MT 59601-5960
Representing: Defendant and Appellant
Service Method: eService

Tammy Plubell
Office of the Montana Attorney General
P.O. Box 201401
Helena, MT 59620-1401
Representing: Plaintiff and Appellee
Service Method: eService

Electronically signed by Krystal Pickens on behalf of Alex Rate
Dated: 12/16/2024

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 12-16-2024:

Mary Leffers Barry (Govt Attorney)
228 Broadway
Lewis & Clark County Attorney Office
Helena MT 59601
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

Kevin Downs (Govt Attorney)
228 E. Broadway
Helena, MT MT 59601
Representing: State of Montana
Service Method: eService

Alexander H. Pyle (Attorney)
Office of the State Appellate Defender
P.O. Box 200147
Helena MT 59620
Representing: Katherine Anne Proctor
Service Method: eService

Karl Pitcher (Attorney)
PO Box 7842
Missoula MT 59802
Representing: The Innocence Network
Service Method: eService

Electronically signed by Krystel Pickens on behalf of Alexander H. Rate

Dated: 12-16-2024