IN THE SUPREME COURT OF THE STATE OF MONTANA
No. DA 24-0139

STATE OF MONTANA

Plaintiff and Appellant,

v.

YANBIN BAO,

Defendant and Appellee.

BRIEF OF APPELLEE

On Appeal from the Montana Fourth Judicial District Court,
Missoula County, The Honorable Leslie Halligan, Presiding

APPEARANCES:

AUSTIN KNUDSEN
Montana Attorney General
ROY BROWN
Assistant Attorney General
215 North Sanders
Helena, MT 59620
Phone: 406-444-2026

ANDREA RENEE HANEY
KATRINA THORNESS
Deputy County Attorneys
Missoula County Courthouse
200 West Broadway
Missoula, MT 59802

ATTORNEYS FOR
PLAINTIFF/APPELLANT

JORDAN KILBY
Stephens Brooke, P.C.
315 W. Pine St.
Missoula, MT 59802
Phone: 406-721-0300

ATTORNEY FOR
DEFENDANT/APPELLEE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases Cited:

Statutes:

Other Authority:

STATEMENT OF THE ISSUES

Whether the district court erred by finding the search of electronic devices was warrantless because Mont. Code Ann. § 46-5-225 requires a warrant be served within 10 days or the warrant is void. Whether the district court erred when it suppressed evidence obtained from the warrantless search.

Alternatively, whether the district court reached the right result for the wrong reason and whether the district court should have suppressed evidence from all the electronic devices.

STATEMENT OF THE CASE

On May 31, 2024, the State of Montana charged Yanbin Bao and Richard Bushey with seven counts of Sex Trafficking, in violation of Mont. Code Ann. § 45-5-702(1) and one count of Labor Trafficking, in violation of Mont. Code Ann. § 45-5-703(1). (Doc. 72, App. A). The State amended the information twice. (Doc. 23, App. B; Doc. 79, App. C). The first amendment corrected legal errors. (Doc. 23, App. B). The second provided a more definite statement of the charges. (Doc. 79, App. C).

On January 22, 2024, Bao filed a motion to suppress all evidence obtained by law enforcement's search of 13 electronic devices seized in Bao and Bushey's case and a related case. (Doc. 54, App. D). The Missoula County Sheriff's Office included all 13 devices in one warrant. (Doc. 54, Ex. A, App. D).

Bao argued Mont. Code Ann. § 46-5-225's 10-day time limit to serve the warrant rendered the warrant void at the time law enforcement searched five of Bao and Bushey's devices. (Doc. 54, App. D) Specifically, the warrant was issued on July 10, 2023, and five devices were not searched until December 2023 and January 2024. (*Id)*

Bao argued the application for the warrant lacked the requisite particularity and did not demonstrate probable cause to search each individual device. Bao argued the search violated Bao's constitutional rights and the evidence should be suppressed. (Doc. 54, App. D).

On February 16, 2024, the district court issued its Order. (Doc. 72, App. A). The Court ordered evidence from four of the devices suppressed but did not suppress the evidence from the remaining 9 devices at issue. *(Id)* The district court held Mont. Code Ann. § 46-5-225 required law enforcement to execute the warrant within 10 days and the searches that occurred in December 2023 and January 2024 fell outside the 10-day time limit. *(Id)*

The State timely filed its notice of appeal. (3/6/24 Notice of Appeal).

STATEMENT OF THE FACTS

Like the district court did in its Order[1], and as required by Mont. R. App. Pro. Rule 12(1)(d), Bao provides facts as they are relevant to the issues on appeal. This is an interlocutory appeal. Bao has not been convicted of the charges before her and therefore retains her presumption of innocence. Nonetheless, the State recited as fact inflammatory and unproven allegations about the charges in the instant case. While Bao is tempted to respond by setting forth her defenses, Bao knows this Court is not swayed by sensational unproven facts. As such, Bao recites only the facts as set forth in the district court's order and will include additional facts relevant to her legal arguments.

The charges in this case arise from a May 29, 2023 call from Jane Doe to 911. (Doc. 72, App. A). Doe reported she was at a local business, Soul Massage in Missoula. (*Id*.) Doe accused Bao and Bushey of running a prostitution and sex trafficking business and stated Bushey assaulted Doe. (*Id*.)

Missoula County Sheriff's Deputies responded. (*Id*.) Deputies arrested Bao and Bushey. (*Id*.) Deputies seized "a cellular phone from Bushey (an Apple iPhone in a black Otter Brand case, LERMS 11) and a separate cellular device from Bao

[1] In a footnote in its order, the district court explained, "Because the present Motion focuses on the evidence connected with electronic devices, the remainder of the recitation of facts shall likewise focus on the seizure and search of the electronic devices as part of the criminal investigation." (Doc. 72).

(an Apple iPhone in a clear case, LERMS 12)." (Doc. 54, Ex. A, App. D). From behind a curtain on a windowsill, deputies seized an Apple iPhone in a purple case (LERMS 13). (Doc. 72, App. A).

Deputies applied for and received a warrant to search the property of Soul Massage. (Doc. 54, Ex. A and B, App. D). The warrant application to search the electronic devices seized stated, "During the search, law enforcement seized 'an Apple iPad Pro in a gray case bearing S/N DMPSMA5YHIMJ (LERMS 14), a red Apple iPhone Pro in a pink and clear case (LERMS 15), a blue Motorola cell phone (LERMS 16), and a black Samsung cell phone bearing IMEI 3513….(LERMS 17)'" (Doc. 54, Ex. A, App. D). The electronic devices seized from Bao and Bushey were identified as LERMS 11-17. (Doc. 72, App. A).

On June 6, 2023, law enforcement arrested another suspect, Hui Wang, with a connection to the allegedly unlawful business at Soul Massage. (Doc. 72, App. A). Law enforcement seized four devices from Wang's purse and two devices within Wang's hotel room. (*Id*.)

On July 10, 2023, law enforcement applied for a single search warrant to search the contents of all 13 seized electronic devices. (*Id*.) The phones were analyzed at varying times between July 2023 and January 2024 by a Forensic Analyst employed by the Sheriff's Department (analyst). (Doc. 54, Ex. D, App. D).

On January 10, 2024, the Missoula County Sheriff's Office notified the prosecutor that "there were issues with the chain of custodies on multiple items for the above case. These issues included incomplete chain of custodies, inaccurate C.O.C's or altogether missing chain of C.O.C.'s….These evidence items in question were the electronic devices along with their corresponding downloads/extractions." (Doc. 54, Ex. C, App. D). On January 16, 2024, the Missoula County Sheriff's Office notified the Missoula County Attorney's Office that the analyst had been placed on administrative leave pending an internal job performance investigation. (*Id*).

In its order suppressing the phones, the district court adopted the timeline set forth in the analyst's report:

> The only timeline of the searches of the 13 electronic devices listed in the search warrant is provided in a report by Forensic Analyst…, a Sheriff's Office employee, attached as Exhibit D to the Motion. That report identifies some of the devices as "LERMS" 11-18. There are some confusing inconsistencies between how the separate devices are identified in Thomas's report and the search warrant, but it appears LERMS 11-1[7] coordinate with the seven devices obtained from Bao, Bushey, and from inside the Soul Massage business. In any case, according to the report, Thomas searched one device, LERMS 11 (Apple iPhone in black Otter brand case), over the course of Jul y 13-19, 2023. She searched another two, LERMS 16 (blue Motorola cell phone) and LERMS 17 (black Samsung cell phone bearing IMEI: 3513…), between July 13-20, 2013 (sic). The report says that Thomas also attempted to search another device, LERMS 14, at 0716 hours on the 20th but was unsuccessful. According to the report

> Thomas did not search the other devices (LERMS 12, 13, 15) until December and January 2024.

(Doc. 72, App. A).

The analyst's report provides information for each device and was attached to the district court briefing as exhibit D. (Doc. 54, Ex. D, App. D). The following comes from that report:

a. LERMS 12

The analyst attempted to search LERMS 12 on July 13, 2023 pursuant to the warrant issued on July 10, 2023. (Doc. 54, Ex. D, App. D). The device was not supported by the search software, GrayKey. (*Id.*)

On January 4, 2024, the analyst again plugged the device into GrayKey and learned that the device was "now supported." (Doc. 54, Ex. D, App. D). She then proceeded to extract data from the phone, conducting a new and distinct search. (*Id.*)

b. LERMS 13

The analyst attempted to search LERMS 13 on July 2023 pursuant to the warrant issued on July 10, 2023. (Doc. 54, Ex. D, App. D). She was unable to use GrayKey to search the device because the device was locked by a passcode. (*Id.*) The analyst initiated the bruteforce process to gain the code and unplugged the device from GrayKey. (*Id).*

On December 1, 2023, after obtaining the password[2], the analyst plugged the phone into GrayKey and extracted data. (*Id.*) On December 5, 2023, the analyst plugged the phone into Cellebrite and performed an additional extraction. (*Id.*)

c. LERMS 14

The analyst made her first attempt to search this device on July 20, 2023. (Doc. 54, Ex. D, App. D). She unplugged the device from Graykey and put the device back in the evidence bag. She removed the device again on December 1, 2023. The disposition of this device is unknown. (*Id.*)

d. LERMS 15

On July 12, 2023, the analyst attempted to extract data from this device. (Doc. 54, Ex. D, App. D). The attempt was unsuccessful. (*Id.*)

On January 5, 2023, the analyst initiated another search of the device by plugging it in to GrayKey. (*Id.*) She was able to extract data from this device. (*Id.*)

The district court suppressed the evidence obtained from the unlawful searches of LERMS 12-15. (Doc. 72, App. A).

[2] The analyst's report does not state when bruteforce was able to obtain the password.

STANDARD OF REVIEW

This Court reviews a district court's "decision on a motion to suppress to determine whether the findings of fact meet the clearly erroneous standard and whether the findings are correctly applied as a matter of law." *State v. Geno*, 2024 MT 142, ¶ 18, 417 Mont. 135; *citing State v. Eskew*, 2017 MT 36, ¶ 12, 386 Mont. 324, 390 P.3d 129. "[T]o the extent a district court's ruling is based on interpretation of a statute, [the Court's] review is *de novo. State v. Kelm*, 2013 MT 115 ¶ 18, 370 Mont. 61, 300 P.3d 687.

SUMMARY OF THE ARGUMENT

Both Article II, Section 11 of the Montana Constitution and the Fourth Amendment to the United States Constitution protect against unreasonable search and seizures such as the searches that occurred in the instant matter. Further, these searches violated Bao's explicit privacy rights conferred to her by Article II, Section 10 of the Montana Constitution.

This Court should uphold the district court's Order suppressing evidence. By applying for one warrant for 13 devices, the Missoula County Sheriff's Office was required to extract the data from all of the devices within 10 days. Mont. Code Ann. § 46-5-225 requires a short time frame to protect citizens from being subjected to unreasonable searches and seizures because the probable cause within a warrant becomes stale as time goes on. In the instant case, the district court correctly interpreted the statute to require law enforcement to copy the data from

the devices within the time frame set forth by the legislature. When law enforcement did not do so, the warrants became void and any subsequent searches were warrantless and violated the United States and Montana's Constitutions.

This Court should not adopt the holdings of other states that do not share Montana's explicit and expanded privacy protections. Other states have essentially carved out an exception to their statutory time frames where there is no evidence that the devices, already in police custody, had been tampered with or that the chains of custody were not intact. Bao urges the Court to give meaning to Montana's heightened privacy rights and not adopt an exception that would swallow the rule.

Should this Court determine an exception to the clear meaning of the statute suffices in Montana, the exception does not apply to these facts. Here, the Court cannot bestow a proper chain of custody and thus the probable cause for a search that occurred six months after the district court granted the warrant was stale. In fact, Bao provided evidence to the district court that the chains of custody were not intact. Therefore, the original warrant would not have applied and any exception this Court may carve out of the time limit in the statute would be inapplicable in the instant case.

Because the search was warrantless and no exception applied, the exclusionary rule applies. No exception to the exclusionary rule applies under these facts. The district court properly suppressed the evidence.

In the alternative, the district court reached the right result for the wrong reason. The application for the warrant did not state with the constitutionally requisite particularity the items to be searched. Further the application did not delineate probable cause to search each device. As such, this Court should hold the district court properly suppressed the four phones at issue and order the evidence from the nine other devices suppressed as well.

ARGUMENT

The Fourth Amendment to the Federal Constitution provides "the rights of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated." U.S. Const. amend IV. Like the Federal Constitution, the Montana Constitution similarly provides that the people shall be free from unreasonable searches and seizures. Mont. Const. Art. II, § 11. In addition, Section 10 of Article II of the Montana Constitution confers additional explicit protections than that of the Federal counterpart. Section 10 states, "the right of individual privacy shall not be infringed without the showing of a compelling state interest."

In 2022, Montana voters amended Montana Constitution's search and seizure provision to explicitly protect "electronic data and communications." Mont. Const. Art. II, § 11. Montana's Declaration of Rights now states:

> The people shall be secure in their persons, papers, *electronic data and communications*, homes and effects from unreasonable searches and seizures. No warrant to search any place, to seize any person or thing, or to access *electronic data or communications* shall issue without describing the place to be searched or the person or thing to be seized, or without probable cause, supported by oath or affirmation reduced to writing.

Mont. Const. Art. II, § 11. (emphasis added to new language). While this Court has historically interpreted Montana's constitutional protections to include electronic devices, this affirmative action underscores Montanan's recognition of the genuine privacy interests people maintain in their electronic devices.

This case involves the unlawful search of electronic devices, namely cell phones. Like in Montana, the Fourth Amendment to the United States Constitution has been interpreted to protect the privacy interests people hold in their cell phones. "Writing for a unanimous Court, Chief Justice Roberts [in *Riley v. California*] noted that modern cell phones contain 'vast quantities of personal information' and are essentially 'digital record[s] of nearly every aspect of their [owners'] lives – from the mundane to the intimate." *Burns v. United States*, 235 A.3d 758, 772 (D.C. Cir 2020) (internal citations omitted) *citing Riley v. California*, 573 U.S. 373 (2014). In reference to the intrusion into a person's

privacy by a search of a cell phone, Chief Justice Roberts further emphasized that the collection of so much varied and sensitive information on a single device, carried almost everywhere by its owner, facilitates in an unprecedented way the "reconstruct[ion]" of "[t]he sum of an individual's private life" and "convey[s] far more" about a person than could previously be found in the search of a physical space. *Riley v California,* at 394, 134 S.Ct. 2473.

"An Internet search and browsing history, for example, ... could reveal an individual's private interests or concerns — perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD." *Id*. at 395-96, 134 S.Ct. 2473. GPS and other historical location information can pinpoint a person's physical location at all times of the day and night, going back weeks, months, and even years. *Id*. at 396, 134 S.Ct. 2473. "And the ever-present mobile applications, known as "apps," "offer a range of tools for managing detailed information about all aspects of a person's life," including political and religious affiliations, banking and other financial matters, addiction treatments, dating and romantic interests, pregnancy milestones, hobbies, and "buying or selling just about anything." *Id*. As a result, "a cell phone search would typically 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." *Id*. at 396-

97, 134 S.Ct. 2473 (emphasis in original); *cf*. *Payton v. New York*, 445 U.S. 573, 589, 100 S.Ct. 1371, 63 L.Ed.2d 639 (1980) (articulating the venerable, pre-*Riley* understanding that Fourth Amendment protections are never "more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home"). See *Burns v. United States*, 235 A.3d 758, 772 (D.C. Cir. 2020).

In addition to the express protections provided to electronic devices, this Court has repeatedly held that Montana's unique constitutional language affords citizens a greater right to privacy generally than the Federal Constitution and therefore provides broader protection than the Fourth Amendment in cases involving searches of private property. *State v. Ellison,* 2000 MT 288 ¶ 46, 302 Mont. 228, 14 P.3d 456. "Independently of the federal constitution, when the right of individual privacy is implicated, Montana's Constitution affords significantly broader protection than the federal constitution." *Weems v. State by & through Knudsen*, 2023 MT 82, ¶ 35, 412 Mont. 132, 149, 529 P.3d 798, 808–09, *citing Gryczan v. State*, 283 Mont. 433, 448, 942 P.2d 112, 121 (1997); *see also Armstrong v. State*, 1999 MT 261, ¶ 34, 296 Mont. 361, 989 P.2d 364. (stating that Montanans right to privacy is the "most stringent" and "exceed[s] even that provided by the federal constitution"). *Weems* interpreted "The delegates to Montana's 1972 Constitutional Convention viewed the textual inclusion of this

right in Montana's new constitution as being necessary for the protection of the individual in 'an increasingly complex society ... [in which] our area of privacy has decreased, decreased, and decreased.'" Montana Constitutional Convention, Verbatim Transcript, March 7, 1972, Vol. V, p. 1681. Delegate Campbell proclaimed that the "right to be let alone" is "the most important right of them all." Montana Constitutional Convention, Verbatim Transcript, March 7, 1972, Vol. V, p. 1681.

Therefore, the federal case law analysis of the Fourth Amendment sets forth the *minimum bar* for analysis of search and seizure and privacy rights in Montana. Not only does Montana law recognize heightened protections for privacy than does the Federal Constitution, but this case also involves electronic communications through cell phones, which in and of themselves garner more protections. Therefore, when the district court was tasked with giving effect to a statute that serves to protect the privacy rights of Montanans through warrant practice, the district court did not err by interpreting the statute in a way that supports these fundamental principles. The district court's decision that the statute at issue supports protecting a person's right to privacy in their cell phone is consistent with the heightened protections afforded by Montana Constitutional law.

I. The district court did not err when it found the searches of the devices were conducted without a warrant.

Four of the seven phones searched by the Missoula County Sheriff's Office analyst were searched without a valid warrant and therefore the searches were unconstitutional intrusions. Warrantless searches are per se unreasonable under the Fourth Amendment of the United States Constitution and the Montana Constitution. *Katz v. United States* (1967), 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576; and *State v. Elison*, 2000 MT 288, ¶ 39; *citing State v. Loh* (1996), 275 Mont. 460, 468, 914 P.2d 592, 597.

Montana statutes govern the procedure for obtaining warrants. Mont. Code Ann. § 46-5-225 states unequivocally:

> The warrant may be served at any time of the day or night. The warrant **must** be served within 10 days from the time of issuance. **Any warrant** not served within 10 days is **void** and must be returned to the court or the judge issuing the warrant and identified as "not served."

(emphasis added).

This Court in *Neely* explained the purpose of the above statute. *State v. Neely* (1993), 261 Mont. 369, 373, 862 P.2d 1109, 1111. "[A]s long as a warrant is executed within ten days from its issuance, as set forth by our legislature in § *46-5-225, MCA*, the warrant itself is not stale." *Id.* Here, the Court found the searches that occurred in January and December were

warrantless searches and violated Bao's federal and Montana constitutional rights.

A. The district court did not err when it interpreted Mont. Code Ann. § 46-5-225, under the current facts, to require a warrant to be executed within 10 days.

The district court correctly interpreted Mont. Code Ann. § 46-5-225. This court should not disturb the district court's interpretation. Because the devices listed in the warrant had already been seized, Mont. Code Ann. § 46-5-225 required law enforcement officers to execute the search commanded by the warrant within 10 days of July 10, 2023. (Doc. 72, App. A). The district court appropriately asked, what other action could the statutory 10-day window govern? (*Id.)*

This court interprets "words and phrases 'according to the context' and, operating under the presumption that the Legislature does not pass meaningless legislation, 'avoid[s] any statutory interpretation that renders any sections of the statute superfluous and does not give effect to all of the words used.' *State v. Ohl*, 2022 MT 241, ¶ 11, 411 Mont. 52, 521 P.3d 759; *citing Belk v. Mont. Dep't of Envtl. Quality*, 2022 MT. 38, ¶ 23, 408 Mont. 1, 504 P.3d 1090 (*internal citations omitted)*. "Words and phrases used in the statutes of Montana are construed according to the context and the approved usage of the language…" Mont. Code Ann. § 1-2-106. "Statutory interpretation 'must be reasonable,' §1-3-233, MCA,

and 'should not lead to absurd results if a reasonable interpretation would avoid it.'" *Ohl*, ¶ 11, *citing State v. Harrison*, 2016 MT 271, ¶ 10, 385 Mont. 227, 230, 383 P.3d 202 (citing *State v. Somers*, 2014 MT 315, ¶ 22, 377 Mont. 203, 339 P.3d 65).

In *Ohl,* this Court found Ohls' interpretation of the escape statute rendered it virtually impossible to commit escape by fleeing detention and would essentially make the statute "meaningless and without effect…" *Ohl*, ¶ 10. This Court held "we will not adopt such an absurd and unreasonable result where reasonable interpretation will avoid it." *Id.*

Here the district court decided not to adopt an absurd interpretation that would give no effect to the statute and instead reasonably interpreted the statute. The State, like *Ohl*, asks this Court to interpret the statute in a way that would render the statute meaningless. The State argues this Court should apply the plain meaning of the word "serve" and that the district court incorrectly determined that serve meant something other than provide service of papers. Following that logic and in order to prevail under it, the State then urges the Court to determine service occurred at the time the judge signed the warrant and provided it to law enforcement.

Interpreting the word "serve" by it's plain meaning would render the statute meaningless under these facts. "The rule of the common law that statutes in

derogation thereof are to be strictly construed has no application to the statutes of the state of Montana. The statutes establish the law of this state respecting the subjects to which they relate, and their provisions and all proceedings under them are to be liberally construed with a view to effect their objects and to promote justice." Mont. Code Ann. § 1-2-103. The devices were in the custody of law enforcement at that time. There was no one to "serve." Certainly, the purpose of "service" of a warrant it so it gives notice to the owner of the device that there is about to be some judicially approved intrusion into the possessor's privacy rights. Reading the statute to mean the warrant shall be served on the entity applying for the warrant is absurd.

In the alternative, the State asks the Court to just determine that the statute does not apply at all: that the court should just ignore the 10-day limit because the object of the search is already in the possession of law enforcement. However, Title 46 of the Montana Code "governs the practice and procedure in **all** criminal proceedings in the Courts of Montana except where provision for a different procedure is specifically provided by law." Mont. Code Ann. § 46-1-103. (emphasis added). The State is unable to offer a different procedure specifically provided by law.

Further, the language of the statute does not except cases where the object of the warrant was already in law enforcement custody. The statute states, "the

warrant must be served within 10 days." Mont. Code Ann. § 46-5-225. And "any warrant not served within 10 day is void…" The statute provides no exception for when a warrant is obtained for items within police custody. Mont. Code Ann. § 46-5-225 thus applies to "any" and therefore all warrants.

The State further argues the 1967 Montana Legislature did not intend for the statutory warrant requirements to apply to electronic devices. However, the delegates of the 1972 Constitutional Convention certainly recognized the need for further protections in "an increasingly complex society…[in which] our area of privacy has decreased, decreased, decreased…" Montana Constitutional Convention, Verbatim Transcript, March 7, 1972, Vol. V, p. 1681. A cell phone search exposes even more information than that of a home search and has long been held to warrant more privacy protections. Even if the 1967 legislature could not have predicted the advent of cellphones, the purpose behind the statute, the protection of privacy, still applies – law enforcement shall not have unbridled access to search property for time immemorial upon the issuance of a warrant.

The district court correctly concluded the warrant was void after 10 days and any search that occurred after that time was done without a warrant. The district court's interpretation of the statute supports the statute's purpose. As the State argues in it's opening brief, the Fourth Amendment, with respect to search warrants, requires "the warrant must….' be based on probable cause, supported by

Oath or affirmation.'" (Appellant Brief p. 36 (June 30, 2024)); citing *Dalia v. United States*, 441 U.S. 238, 255 (1991) and Mont. Code Ann. § 46-5-221. Compliance with Mont. Code Ann. § 46-5-225 for all warrant guarantees the probable cause within the application is not stale and underscores the constitutional requirement that probable cause is a necessary to protect citizens' privacy.

B. The July 10, 2023 warrant used to search the devices was void and therefore the distinct searches that occurred in December and January were unlawful.

Here, the Court correctly determined the analyst did not have a valid warrant to conduct the searches. The warrant previously used was void on July 20, 2023. The federal corollary to Mont. Code Ann. § 46-5-225 is instructive. It contains specific language addressing electronically stored information that the Montana legislature has not adopted. However, the language dictates how time limits should apply and takes into account the constitutional requirement that the probable cause in warrants remain valid. Fed. R. Crim Pro. Rule 41(e)(2) states, in pertinent part:

> (A)…The warrant must command the officer to:
>
> (i) execute the warrant within a specified time no longer than 14 days;…
>
> (B) *Warrant Seeking Electronically Stored Information.* A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Notably here, the federal rule's language supports the district court's interpretation of Mont. Code Ann. § 46-5-225. Specifically, the federal rule explains that the time limit refers to the "seizure of evidence or on-site copying of the media information." Pursuant to the federal rule, satisfaction of the time limit occurs when law enforcement seizes the evidence within the time limit. Media evidence already in law enforcement possession must be copied within the time frame set forth by the statute.

Although Montana has not adopted this language, the intent of the rules are the same – to prevent the warrant from becoming stale and therefore, the acts ordered in the warrant are executed in a timeframe to accomplish that goal. Here the evidence must be copied (i.e. an image made of the device often referred to as the data extracted) within 10 days. Bao is not arguing the search of the extraction needed to occur within 10 days, only that the evidence must have been copied in that time.

The analyst handled the devices on many different occasions from July 2023-January 2024. She found that she did not have the software she needed to extract data from some of the devices during her first attempts in July. At the point at which the analyst attempted to extract the data and that search was unsuccessful, the warrant should have been returned as "not served" pursuant to Mont. Code

Ann. § 46-5-225. This did not occur because law enforcement decided to use one single warrant for 13 devices. This decision does not change the fact that when the analyst then had the software update that worked on the devices and used it six months later, a separate search occurred.

Imagine law enforcement received a warrant to search a home. Within the home, law enforcement located a locked basement door. At the time of the search, law enforcement did not have the tools to open the door. Could law enforcement return six months later to open the door with the proper tools? Could law enforcement return 11 days later? The State will likely respond that, unlike the basement in the example here, the phones were in law enforcement custody for the entire time. However, the forensic technician did not maintain the chain of custody of the evidence. The Court cannot therefore bestow the assumption that the item remained unchanged and that probable cause for the initial warrant remained in tact. That again, would lead to an absurd result.

The act of plugging a phone into software is a search of the phone. The use of GrayKey and Cellebrite constitute separate searches of the phones and they are separate software programs that require separate acts. The extraction of the data from the phones constitutes a seizure. The devices at issue were not searched nor was the data seized before the warrant was void. A separate warrant was required to initiate new searches of the phones in December; at the very least to protect

Bao's privacy rights and ensure that probable cause existed to search the phones after they had been in police custody for four to five months.

Because the analyst searched the devices anywhere from four to five months after the expiration of the July 10, 2023 warrant, the searches were warrantless and the district court did not err when it suppressed the evidence.

C. The purpose of Mont. Code Ann. § 46-5-225 is to ensure that the probable cause in the warrant is not stale and the search in the instant case exceeded the probable cause articulated in the application because, under the facts, the execution of the warrant months after it was issued rendered the warrant stale.

Cases analyzing the federal rule which specifically articulate a "later review" of the data, rely on the principle that the probable cause in the warrant is not stale because presumably the devices have been secured in police custody and the chain of custody is intact. *United States v. Castro*, 881 F.3d 961, 966 (6th Cir. 2018) *citing United States v. Evers*, 669 F.3d 645, 650–52 (6th Cir. 2012) (holding officers may conduct a more detailed search of an electronic device after it was properly seized so long as the later search does not exceed the probable cause articulated in the original warrant and the device remained secured.)

Additionally, the analysis from the out-of-state cases cited by the State all turn on the issue of insuring probable cause is not stale. *See People v. Shinohara*, 375 Ill. App. 3d 85, 104, 872 N.E.2d 498, 516 (2007) ("We emphasize the purpose of statutes invalidating search warrants for delay in execution is to insure that the

items sought by the warrant are in the place to be searched, that probable cause supporting the search warrant has not grown stale and that the integrity of the evidence has not been compromised."); *State v. Monger*, 306 Ore. App. 50, 61, 472 P.3d 270, 276 (2018) ("It seems desirable to keep the time allowed for execution of search warrants as short as possible. This tends to eliminate problems with respect to staleness of the warrant which often form a fruitful basis for attack on the legality of the warrant."); *State v. Nadeau*, 2010 ME 71, ¶ 48, 1 A.3d 445 (finding "the officers in this case were already in possession of the computer at the time the warrant was issued" and thus, "the warrant…was effectively executed at the time it was issued, and there was no danger that the search for the computer conducted after the expiration of the ten-day period would result in a seizure based on stale probable cause.");

Specifically in *State v. Monger*, the Court of Appeals of Oregon reasoned that the subsequent search of a phone "that had been stored in an evidence room" and where the detective "did not interact with the devices in any capacity, " did not violate the principle behind the statute when the device had been undisturbed. *Monger* 306 Ore. App. at 53, 61. That is not the case here.

Although the district court's decision that the warrant was void after 10 days and the searches were warrantless did not necessitate the district court make a finding with regard to the chain of custody, Bao argued the chain of custody with

regard to the devices at issue was not intact as evidenced by the letter attached to Doc. 54 as Sealed Exhibit C. Therefore, not only were the warrants executed outside of the clear 10-day time limit, but the probable cause within the initial application is stale given the mishandling of the devices. At the time the Court made its decisions, the person responsible for their care was on administrative leave due to her conduct with respect to these specific devices.

A separate warrant was required to initiate new searches of the phones in December; at the very least to protect Bao's privacy rights and ensure that probable cause existed to search the phones after they had been in police custody for four to five months. The phones had been turned on; they had been moved. Some had been altered and placed into different "modes." Pursuant to the letter from the Sheriff's Department, the chain of custody was "missing." The warrantless search of the phones violated Bao's right to be free from unreasonable search and seizure, as well as her right to privacy. As such, the evidence obtained therefrom should be suppressed.

D. This Court should not adopt other State's reasoning, which would invalidate the language of Mont. Code Ann. § 46-5-225.

The State erroneously relies on caselaw from other states asking this Court to find the search of an electronic device can occur any time after the warrant is issued. Montanans enjoy more privacy than those in other States and therefore the analysis should not apply to the case at hand.

The State cites cases from New Mexico, New York, Pennsylvania, Oregon, Wisconsin, and Illinois. The cases cited can be differentiated from the case here. Several of the States relied on by the State do not have language in the statutes specifically rendering a warrant void after the time frame. See ORS 133.565(3); Pa.R.Crim.P 205; N.M.R.Crim.P. 5-211(C).

In the case most relied upon by the State, *People v. Shinohara*, the issue was whether a subsequent search of the data extracted from a phone violated Illinois's similar (but not the same) statute limiting execution of warrants to 96 hours. *Shinohara*, 375 Ill. App. 3d 85, 104, 872 N.E.2d 498, 516 (2007) In *Shinohara*, the detective created a mirror image (an extraction) of the computer within the time frame – the day after the warrant was issued. *Id.* at 102. The Court found the detective "executed the warrant by completely carrying out the directions…when he made a mirror image copy of defendant's hard drive." *Id.* The Court went on to analyze whether a delay would have affected Defendant's rights under the Fourth Amendment and held "A delay in the execution of a search warrant does not violate a defendant's right to be free from an unreasonable search *absent a showing of the interim dissipation of probable cause or any prejudice to the defendant." Id.* at 107. (emphasis added).

Like in *Shinohara*, the analyst does the same when she extracts the data – makes a mirror image of the phone. She did not do so within the time frame of the

warrant and therefore the warrant was void. Additionally, the *Shinohara*'s fourth amendment analysis is just the threshold analysis for cases in Montana and because one cannot assume the probable cause was intact here, the evidence from the warrantless search should be suppressed.

Montanans' right to privacy has been a source of pride for Montana's legal scholars, judges and attorneys throughout the State. Just because other States have interpreted their statutes (which are different) in ways which do not protect their citizens, does not mean that Montana should follow suit under a completely different Declaration of Rights and body of caselaw. The district court interpreted Montana's statute explicitly voiding a warrant not served within 10 days in accordance with Montana's history of bestowing more privacy upon its citizens than the federal government or even its neighbors. As such this Court should view with caution analyses from other states.

II. Application of the exclusionary rule is appropriate in this case.

Because the search violated Bao's constitutional rights, the exclusionary rule applies. The exclusionary rule ensures protection against the government's intrusion on an individual's constitutional right to be free from such unreasonable searches and seizures. *Wong Sun*, 371 U.S. at 485, 83 S. Ct. at 416. If a warrant was constitutionally required, and a search occurred without a warrant and an exception to the warrant requirement is not established, the evidence obtained as a

result of an unreasonable search or seizure is excluded. *Wong Sun v. U.S.*, 371 U.S. 471, 484-85, 83 S. Ct. 407, 416, 9 L. Ed. 2d 441 (1963). "The exclusionary rule bars evidence obtained as a result of an unconstitutional search or seizure, also known as "fruit of the poisonous tree," and is the primary vehicle which helps to ensure protection from an unreasonable governmental search or seizure." *State v. Dickinson,* 2008 MT 159, ¶ 19*, citing State v. Ottwell*, 239 Mont. 150, 154, 779 P.2d 500, 502 (1989).

The State argues the facts only constitute a technical violation of a statute and not a constitutional violation invoking the exclusionary rule. The State ignores the language of the statute violated that explicitly states, the warrant is **void** if not served within 10 days. Mont. Code Ann. § 46-5-225 (emphasis added). Pursuant to *Neely*, the statute protects the probable cause upon which the warrant was issued from becoming stale. Here, the State is unable to show the probable cause was not stale. As the State cited in it's brief, the Fourth Amendment requires a warrant to search an electronic device and also requires the warrant be issued on probable cause. (Appellant Brief p. 37 (June 30, 2024)). The remedy for a Fourth Amendment violation is exclusion of the evidence.

This Court has declined to apply the good faith exception to the warrant application and should not do so here. *See State v. Stewart*, 2012 MT 317, 367 Mont. 503, 291 P.3D 1187. Here, the analyst could not act on good faith as she

was the person responsible for the chain of custody of the phones, essentially responsible for keeping the probable cause intact. She did not do so and therefore the search was made on a void warrant. If the warrant is void and the search is warrantless, the exclusionary rule applies.

III. Alternatively, the district court came to the right result for the wrong reason and therefore should have suppressed evidence from all of the devices because the warrant application was unconstitutionally general.

The warrant clause of the Fourth Amendment commands that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." U.S. Const. amend. IV. "[These words] reflect the determination of those who wrote the Bill of Rights that the people of this new Nation should forever 'be secure in their persons, houses, papers and effects' from intrusion and seizures by officers acting under the unbridled authority of a general warrant." *Stanford v. Texas*, 379 U.S. 476, 481, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965). The affidavit "must establish a nexus between the place to be searched and things to be seized, such that there is a substantial basis to believe that the things to be seized will be found in the place searched." *Ellison v. Balinski,* 625 F.3d 953, 958 (6th Cir.2010).

Although Article II, Section 11 of the Montana Constitution omits the word "particularly," this Court has held that the Montana Constitution imposes a particularity requirement identical to that under the United States

Constitution. *See State v. Ballew* (1973) 163 Mont. 257, 261, 516 P.2d 1159, 1161-62 (citation omitted). Further, Montana statute provides the following grounds for a search warrant:

> A judge shall issue a search warrant to a person upon application, in writing, by telephone, or electronically, made under oath or affirmation, that:
>
> (1) states facts sufficient to support probable cause to believe that an offense has been committed;
>
> (2) states facts sufficient to support probable cause to believe that evidence, contraband, or persons connected with the offense may be found;
>
> (3) particularly describes the place, object, or persons to be searched; and
>
> (4) particularly describes who or what is to be seized.

Mont. Code Ann. § 46-5-221.

A. The warrant in this case did not state, with the required particularity, the evidence for which the investigator was searching; instead, it included a laundry list of items which authorized law enforcement to take a constitutionally unauthorized deep dive into the devices and as such the evidence obtained must be suppressed.

The Fourth Amendment to the United States Constitution and Article II, Section 11 of the Montana Constitution require in part that a search warrant particularly describe the items it authorizes to be seized. Additionally, § 46-5-221(4), MCA, states in relevant part that "[a] judge shall issue a search warrant to a person upon application ... made under oath or affirmation, that ... particularly describes who or what is to be seized." This requirement of particularity serves to

prevent a "general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire* (1971), 403 U.S. 443, 467, 91 S.Ct. 2022, 2038, 29 L.Ed.2d 564, 583. " 'As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.' " *Stanford v. Texas* (1965), 379 U.S. 476, 485, 85 S.Ct. 506, 511, 13 L.Ed.2d 431, 437 (quoting *Marron v. United States* (1927), 275 U.S. 192, 196, 48 S.Ct. 74, 76, 72 L.Ed. 231, 237) see also *State v. Seader*, 1999 MT 290, ¶ 11, 297 Mont. 60, 63, 990 P.2d 180, 182.

This Court, in analyzing the above passage from *Marron*, stated:

> Observers have frequently remarked that the passage from *Marron* cannot be read literally because few warrants would survive such a stringent rule. *See, e.g., State v. Perrone* (1992), 119 Wash.2d 538, 834 P.2d 611, 615. *See also* 2 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment, § 4.6(a) (3d ed.1996). In *Perrone,* the court found that "the warrant must enable the searcher to reasonably ascertain and identify the things which are authorized to be searched." 834 P.2d at 615 (citations omitted). "The common theme of all descriptions of the particularity standard is that the warrant must allow the executing officer to distinguish between items that may and may not be seized." *United States v. Leary* (10th Cir.1988), 846 F.2d 592, 600 n. 12.
>
> The specificity required of a search warrant may vary depending on the circumstances of the case and the type of items involved. Generic categories or general descriptions of items are not necessarily invalid if a more precise description of the items to be seized is not possible. *See United States v. Spilotro* (9th Cir.1986), 800 F.2d 959, 963 (citations omitted); *Perrone,* 834 P.2d at 616 (citations omitted).

State v. Seader, 1999 MT 290, ¶¶ 11-13, 297 Mont. 60, 63, 990 P.2d 180, 182–83

Nonetheless, "General searches have long been deemed to violate fundamental rights." *Marron v. U.S.* 275 U.S. 192, 194 (1927). The condition for

particularity guarantees the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit. *Maryland v. Garrison*, 480 U.S. 79, 84, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987). In obligating officers to describe the items to be seized with particularity, the Fourth Amendment prevents "the issu[ance] of warrants on loose, vague or doubtful bases of fact." *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357, 51 S.Ct. 153, 75 L.Ed. 374 (1931).

The Ninth Circuit recognized warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible. *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986), *citing United States v. Cardwell,* 680 F.2d 75, 78 (9th Cir.1982). In determining whether a description is sufficiently precise, the Ninth Circuit concentrates on one or more of the following: (1) whether probable cause exists to seize all items of a particular type described in the warrant, *see, e.g., United States v. McClintock,* 748 F.2d 1278 at 1283; *United States v. Offices Known as 50 State Distributing Co.,* 708 F.2d 1371, 1374 (9th Cir.1983), *cert. denied,* 465 U.S. 1021, 104 S.Ct. 1272, 79 L.Ed.2d 677 (1984); (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not, *see, e.g., United States v. Pollock,* 726 F.2d 1456, 1466 (9th Cir.1984); *United States v. Gomez-Soto,* 723 F.2d 649 at 653–54; *United States*

v. Cardwell, 680 F.2d 75 at 78; *United States v. Hillyard,* 677 F.2d 1336 at 1340; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued, *Id. citing Cardwell,* 680 F.2d at 78; *Hillyard,* 677 F.2d 1336 at 1339–40. *United States v. Cortellesso,* 601 F.2d 28, 32 (1st Cir.1979), *cert. denied,* 444 U.S. 1072, 100 S.Ct. 1016, 62 L.Ed.2d 753 (1980).

In *Spilotro*, the Ninth Circuit reversed the district court in concluding "the warrants did not describe the items to be seized with sufficient particularity, and the Court could not conscientiously distinguish this case from others in which [the Court has] held warrants invalid because of their general terms. *See, e.g., United States v. Cardwell,* 680 F.2d 75 (9th Cir.1982); *VonderAhe v. Howland,* 508 F.2d 364 (9th Cir.1974) (civil action contesting warrant executed by IRS)." The warrants authorized a search for:

> notebooks, notes, documents, address books, and other records; safe deposit box keys, cash, and other assets; photographs, equipment including electronic scanning devices, and other items and paraphernalia, which are evidence of violations of 18 U.S.C. 1084, 1952, 892–894, 371, 1503, 1511, 2314, 2315, 1962–1963, and which are or may be: (1) property that constitutes evidence of the commission of a criminal offense; or (2) contraband, the fruits of crime, or things otherwise criminally possessed; or (3) property designed or intended for use or which is or has been used as the means of committing a criminal offense.

Spilotro, 800 F.2d at 961-2. The Court stated, "the government could have narrowed most of the descriptions in the warrants either by describing in greater detail the items one commonly expects to find on premises used for the criminal activities in question, or, at the very least, by describing the criminal activities themselves rather than simply referring to the statute believed to have been violated. As the warrants stand, however, they authorize wholesale seizures of entire categories of items not generally evidence of criminal activity, and provide no guidelines to distinguish items used lawfully from those the government had probable cause to seize." *Spilotro*, 800 F.2d 959, 963–64 (9th Cir. 1986).

In Montana's *State v. Seader*, the search warrant application stated that the police had probable cause to believe the offense of Criminal Possession of Dangerous Drugs had been committed and that drugs and drug-related evidence would be found in Seader's van. Additionally, the warrant had the language "anything else of value furnished or intended to be furnished in the exchange for the evidence or contraband relating to the use, sale or manufacture of dangerous drugs." *Seader*, ¶ 7. The warrant in part authorized the seizure of "proceeds of drug sales whether in monies, precious metals, property or anything else of value furnished or intended to be furnished in the exchange for the evidence or contraband relating to the use, sale or manufacture of dangerous drugs." *Id*.

In reversing the district court, this Court held the search warrant was not sufficiently particular with respect to the items subject to seizure to meet the requirement of particularity, stating the "anything else of value" rendered the warrant facially overbroad and all evidence pursuant to it "was inadmissible and should have been suppressed." *Id*, ¶ 16.

A case interpreting federal law from the District of Columbia Court of Appeals is informative. In *Burns v. United States,* the government obtained a warrant that authorized a search of one phone for "all records" and "any evidence" on the device that relate to the crime of homicide. *Burns v. United States*, 235 A.3d 758. The warrants did not limit the police to a search of the data for which the police had probable cause to search, but, like in the instant case, authorized a review of the entire contents of the phone.

In reversing the trial court, the D.C. Circuit stated:

> In any context, a search warrant's "general description" of items to be seized, such as "records, mail, correspondence, and communications is immediately suspect as being upon nothing more than conjecture that such items related to the crime under investigation actually exist. 2 Wyne R. LaFave, *Search & Seizure* § 4.6(a) (5th ed. 2012 & 2019 update) (internal quotation marks omitted). Particularly given the heightened privacy interests attendant to modern smart phones under *Riley*, it is thus constitutionally intolerable for search warrants simply to list generic categories of data typically found on such devices as items subject to seizure.

Burns, 235 A.3d at 775. The Court held the warrants were overbroad and lacked particularity and probable cause. *Id.*

The warrant in the instant case is overbroad and only generally describes the evidence to be seized. The warrant begins by listing ten items which only apply to computers (e.g. “”Evidence of who used, owned, or controlled the computer at the times the thigs described in this warrant were created, edited or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat” instant messaging logs, photographs, and correspondence….Evidence of the attachment to the computer of other storage devices or similar containers of electronic devices….Records of or information about Internet Protocol addresses used by the computer,” etc.) (Doc. 54, Ex. A) In addition to the list of inapplicable data to be extracted from computers, the warrant allows for seizure of the following laundry list of data and includes the term “all data”:

All data currently stored in or related to the account or device identified herein related to the crimes or offenses identified herein, including but not limited to:

- Global or regional navigation satellite system data, including data from the Global Positioning System (GPS), Global Navigation Satellite System (GLONASS), BeiDou Navigation Satellite System (BDS), and similar systems;
- Latitude and longitude data;
- Location history,
- IP addresses;
- Activity history or logs;
- Address book or calendar data;
- Contact forwarding data;
- Photographs, audio or video files;
- Metadata;
- Email messages and attachments;
- Documents or other text-based files;
- Timeline history;
- Public profiles;
- Login history;
- Browsing or search history;
- Visited websites;
- Text messages (SMS);
- Media messages (MMS);
- Instant messages;
- Privacy settings;
- Account information, including any linked financial or credit card accounts;
- Any data on a linked social media or communication account or application.

The warrant is overbroad, general, and does not comport with the constitutional requirements that warrants state with particularity the items to be seized. The language allows for a wholesale search of all the devices without judicial limit on what specific evidence is sought. The warrant does not allow the executing officer to distinguish between items that may or may not be seized because it allows for seizure of "all data…including but not limited to…" followed by a list. There are no objective standards in the warrant that guide the search.

The officer was, nonetheless, able to specify. The warrant application and warrant do not state things like "files that depict advertisements for prostitution," or "text messages between Bao and the complaining witnesses," or "text messages between Bao and customers."

Further, the application could have explained that it would be searching for web history about posting the advertisements that are alleged to be tied to the phones. The application could have explained that it was looking to search messaging applications for "group chats."

Deputies knew on May 29, 2023, that Jane Doe and Bao communicated on an application called "We Chat." (Doc. 54, App. D) The application for the warrant did not contain this information nor state with particularity that only "We Chat" should be searched for their conversations. (Doc. 54, Ex. A, App. D). Instead, the application was for a wholesale search of all the contents of the phone.

Additionally, the warrant allows for a search of the phone dating farther back than when the offense is alleged to have occurred, in spite of law enforcement's knowledge of when the victim was at the property. Law enforcement certainly could have put a time limit in the application – that was not impossible.

Like the warrants in *Spilotro, Seader,* and *Burns,* the warrant here does not describe with particularity the evidence to be seized, but authorizes wholesale seizures of entire categories of information. The language "all data…related to the crime," is the same as the offending language in *Spilotro* that states generally "property that constitutes evidence of the commission of a criminal offense" and the language in *Burns* of "all records." The "all data" language allows the officers indiscriminate access to the most intimate details of a person's life.

Here, the language of the warrant is facially overbroad and like in *Seader*, the district court should have suppressed evidence from all devices. This warrant does not meet the federal constitutional and Montana constitutional and statutory requirement that the warrant state with particularity what items are to be seized.

B. The warrant application did not state facts sufficient to support probable cause to believe that evidence or contraband connected with the offense would be found on the devices.

"The requirement of particularity is closely tied to the requirement of probable cause." 2 LaFave, *Search & Seizure* § 4.6(a). When a warrant describes the objects of the search in unduly "general terms," it "raises the possibility that

there does not exist a showing of probable cause to justify a search for them." *Id.* § 4.6(d). A judge reviewing a warrant application must determine, after consideration of the totality of the circumstances, whether the affidavit provides evidence to show "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). An affidavit that states only "suspicions, beliefs, or conclusions, without providing some underlying factual circumstances regarding veracity, reliability, and basis of knowledge, is a 'bare bones' affidavit and fails to establish probable cause." *United States v. West*, 520 F.3d 604, 610 (6th Cir. 2008).

In *Morales*, a case from the US Army Court of Criminal Appeals, police investigating a sexual assault applied for a warrant for a phone they seized from the chief suspect in the case. *United States v. Morales*, 77 M.J. 567, 571 (A. Ct. Crim. App. 2017). The affidavit described an inculpatory text message the suspect sent to the complainant, but it presented no other facts to establish a nexus between the alleged assault and any other data that might be found on the phone. *Id*. The warrant nonetheless authorized a forensic examination of all of the phone's digital data, and in the course of the ensuing search, police reviewed a photo-editing application on the phone and came across three photographs of the assault as it was being committed. *Id*. at 571-72. In reversing the trial court, the appellate court held although the affidavit made out probable cause to search the defendant's text

messages, the affidavit "provided no factual predicate" to search for photographs "and no factual basis to conduct an open-ended search of the phone's entire contents." *Id*. at 577. As here, the warrant violated the probable cause and particularity requirements of the Warrant Clause. *Id*. at 575. See also *Burns*, at 776.

Here, like in *Morales,* there is no nexus between the information in the affidavit and the specific devices. In fact, the warrant application in *Morales* contained more probable cause because the *Morales* application listed a specific text message that would be on the phone. But here, the only language that suggests evidence may be found on the phone in the application is unconstitutionally general and states, *"Criminals will often use voicemail messages, text messages, picture messages, and other wireless communication methods to facilitate their crimes."* (Doc. 54, Ex. A, App. D). This language does not provide the court with enough information to determine if there is actual probable cause that the laundry list of items will be found on the devices and that those things will be actual evidence of the crime alleged. Nor does the language support probable cause that evidence of the instant offense will be found on the devices. The warrant does not contain any language regarding the specific crime of human trafficking and how the devices may have been used in furtherance of the crime. That a phone was found on a person and that person is alleged to have committed a crime and a

general statement that criminals use voicemail messages, text messages, picture messages and other wireless communication methods to facilitate their crimes – does not rise to probable cause.

The warrant generally sets forth an allegation that Bushey and Bao were engaged in human trafficking, which satisfies Mont. Code Ann. § 46-5-221(1), but the warrant does not establish "facts sufficient to support probable cause to believe that evidence [or] contraband…connected with the offense may be found" as required by Mont. Code Ann. § 46-5-221(2). Therefore, the evidence extracted from the devices should be suppressed.

CONCLUSION

For the foregoing reasons Bao requests the Court not disturb the district court's decision to suppress the evidence obtained from the electronic devices. Should the Court find the district court reached the right result for the wrong reasons, the Court should remand and order the district court to suppress the evidence from the 9 remaining devices. The searches in this case violated Bao's rights to be free from unreasonable searches and seizures and her explicit right to privacy.

Respectfully submitted this 31st day of July, 2024.

STEPHENS BROOKE, P.C.

/s/ Jordan Kilby
Jordan Kilby
Attorney for Defendant and Appellee
Yanbin Bao

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 11 of the Montana Rules of Appellate Procedure, I certify that this response brief is printed with a proportionately spaced Times New Roman text typeface of 14 points; is double spaced except for footnotes and for quote and indented material; and the word count calculated by Microsoft Word for Windows is 9892 words, excluding cover page, table of contents, table of authorities, certificate of service, certificate of compliance, signatures and any appendices.

/s/ Jordan Kilby
Jordan Kilby

CERTIFICATE OF SERVICE

I, Jordan Rhodes Kilby, hereby certify that I have served true and accurate copies of the foregoing Brief - Appellee's Response to the following on 07-31-2024:

Andrea Renee Haney (Govt Attorney)
200 West Broadway
Missoula MT 59802
Representing: State of Montana
Service Method: eService

Roy Lindsay Brown (Govt Attorney)
Appellate Services Bureau
Attorney General's Office
215 N Sanders St
P.O. Box 201401
Helena MT 59601
Representing: State of Montana
Service Method: eService

Electronically signed by Courtney Johnson on behalf of Jordan Rhodes Kilby
Dated: 07-31-2024