

SUPREME COURT
STATE OF COLORADO

2 East 14th Avenue
Denver, CO 80203

On Certiorari to the Colorado Court of Appeals
Court of Appeals Case No. 20CA1565

KEVIN MATTHEW DHYNE,
Petitioner

v.

THE PEOPLE OF THE
STATE OF COLORADO

Respondent.

PHILIP J. WEISER, Attorney General
TRINA K. KISSEL, Senior Assistant
Attorney General*
Ralph L. Carr Colorado Judicial Center
1300 Broadway, 9th Floor
Denver, CO 80203
Telephone: 720-508-6400
E-Mail: AG.Appellate@coag.gov
Registration Number: 47194
*Counsel of Record

▲ COURT USE ONLY ▲

Case No. 22SC869

ANSWER BRIEF

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with all requirements of C.A.R. 28 or C.A.R. 28.1, and C.A.R. 32, including all formatting requirements set forth in these rules. Specifically, the undersigned certifies that:

The brief complies with the word limits set forth in C.A.R. 28(g) or C.A.R. 28.1(g).

It contains 9,335 words (principal brief does not exceed 9500 words; reply brief does not exceed 5700 words).

The brief complies with the standard of review requirements set forth in C.A.R. 28(a)(7)(A) and/or C.A.R. 28(b).

It contains under a separate heading (1) a concise statement of the applicable standard of appellate review with citation to authority; and (2) a citation to the precise location in the record (R. , p.), not to an entire document, where the issue was raised and ruled on.

I acknowledge that my brief may be stricken if it fails to comply with any of the requirements of C.A.R. 28 or 28.1, and C.A.R. 32.

s/ Trina K. Kissel _____

TABLE OF CONTENTS

	PAGE
INTRODUCTION	1
STATEMENT OF THE FACTS AND THE CASE.....	2
I. The investigation.....	2
II. Trial court proceedings	4
III. The appeal	7
SUMMARY OF THE ARGUMENT.....	8
ARGUMENT.....	10
I. Law enforcement reasonably concluded that the warrant authorized a search of Dhyne’s room.	10
A. Preservation and standard of review.....	10
B. Relevant law	13
1. Facial validity of a warrant	13
2. Reasonableness of a warrant’s execution.....	14
C. Analysis	19
1. The warrant was facially valid.....	20
2. The detective’s execution of the search warrant was lawful.	23
3. Dhyne’s concerns about probable cause from shared internet are not preserved or pertinent to this case.	37
II. Alternatively, the trial court properly applied the inevitable discovery exception to the exclusionary rule.	43
A. Preservation and standard of review.....	43
B. Relevant law	44
C. Analysis	46
1. Discovery of the evidence was inevitable.....	46

TABLE OF CONTENTS

	PAGE
2. This Court should not adopt a different formulation of the inevitable discovery exception.....	50
CONCLUSION	55

TABLE OF AUTHORITIES

CASES	PAGE
<i>Booth v. Antill</i> , 849 F.2d 604 (4th Cir. 1988)	18
<i>Brierley v. City</i> , 390 P.3d 269 (Utah 2016)	52
<i>Casillas v. People</i> , 2018 CO 78M	45
<i>Commonwealth v. Molina</i> , 71 N.E.3d 117 (Mass. App. Ct. 2017)	27
<i>Doe v. Olson</i> , 691 F. App'x 272 (8th Cir. 2017)	28
<i>Illinois v. Rodriguez</i> , 497 U.S. 177 (1990)	23
<i>In re Warrant Application</i> , No. 22 M 00595, 2023 WL 1878636 (N.D. Ill. Feb. 1, 2023)	26
<i>Jeffers v. Commonwealth</i> , 743 S.E.2d 289 (Va. Ct. App. 2013) ..	27, 34, 35
<i>Maryland v. Garrison</i> , 480 U.S. 79 (1987)	passim
<i>Missouri v. McNeely</i> , 569 U.S. 141 (2013)	34, 42, 52
<i>Muhammad v. Pearson</i> , 900 F.3d 898 (7th Cir. 2018)	14, 15
<i>Nix v. Williams</i> , 467 U.S. 431 (1984)	45, 46, 50, 54
<i>People v. Avery</i> , 173 Colo. 315, 478 P.2d 310 (1970)	14
<i>People v. Burola</i> , 848 P.2d 958 (Colo. 1993)	46
<i>People v. Cooper</i> , 2016 CO 73	13
<i>People v. Dhyne</i> , 2022 COA 122	passim
<i>People v. Diaz</i> , 53 P.3d 1171 (Colo. 2002)	49
<i>People v. Fields</i> , 2018 CO 2	46
<i>People v. Lucero</i> , 174 Colo. 278, 483 P.2d 968 (1971)	16, 17
<i>People v. Martinez</i> , 165 P.3d 907 (Colo. App. 2007)	17, 24

TABLE OF AUTHORITIES

	PAGE
<i>People v. McKay</i> , 2021 CO 72.....	10
<i>People v. McKnight</i> , 2019 CO 36.....	54
<i>People v. Mershon</i> , 874 P.2d 1025 (Colo. 1994)	11, 12
<i>People v. Morehead</i> , 2019 CO 48.....	10
<i>People v. Nguyen</i> , 12 Cal. App. 5th 574 (2017).....	28, 39, 40
<i>People v. Roccaforte</i> , 919 P.2d 799 (Colo. 1996)	15
<i>People v. Syrie</i> , 101 P.3d 219. (Colo. 2004).....	46
<i>People v. Tallent</i> , 2021 CO 68	45
<i>People v. Ward</i> , 181 Colo. 246, 508 P.2d 1257 (1973)	17
<i>People v. Webb</i> , 2014 CO 36	17
<i>Peters v. State</i> , 120 A.3d 839 (Md. Ct. Spec. App. 2015).....	18
<i>Ramirez v. Webb</i> , 835 F.2d 1153 (6th Cir. 1987).....	18
<i>Rodriguez v. State</i> , 187 So. 3d 841 (Fla. 2015).....	51
<i>State v. Hawkins</i> , 201 P.3d 239 (Ore. Ct. App. 2009)	18
<i>State v. Nieto</i> , 993 P.2d 493 (Colo. 2000).....	44
<i>State v. Patmon</i> , 604 P.2d 82 (Kan. Ct. App. 1979)	18
<i>State v. Teague</i> , 469 So. 2d 1310 (Ala. Crim. App. 1985)	18
<i>United States v. Aljabari</i> , 626 F.3d 940 (7th Cir. 2010)	14, 15
<i>United States v. Axelrod</i> , No. WDQ-10-0279, 2011 WL 1740542 (D. Md. May 3, 2011).....	31, 32, 33
<i>United States v. Ayala</i> , 646 F. Supp. 3d 1191 (N.D. Cal 2022)	29
<i>United States v. Butler</i> , 793 F.2d 951 (8th Cir. 1986).....	18
<i>United States v. Cooper</i> , 24 F.4th 1086 (6th Cir. 2022).....	49

TABLE OF AUTHORITIES

	PAGE
<i>United States v. Cunningham</i> , 413 F.3d 1199 (10th Cir. 2005)	52
<i>United States v. Gilman</i> , 684 F.2d 616 (9th Cir. 1982)	18
<i>United States v. Houck</i> , 888 F.3d 957 (8th Cir. 2018)	35
<i>United States v. Huntoon</i> , No. R1600046001TUCDCBDTF, 2018 WL 1755788 (D. Ariz. Apr. 12, 2018)	27
<i>United States v. Johnson</i> , 26 F.3d 669 (7th Cir. 1994)	18
<i>United States v. Kaplan</i> , 526 F. Appx. 208 (3d Cir. 2013).....	18
<i>United States v. Lewis</i> , 62 F.4th 733 (2d Cir. 2023)	34
<i>United States v. Mejia</i> , No. 08 CR 1019, 2012 WL 4434367 (N.D. Ill. Sept. 24, 2012).....	47, 48
<i>United States v. Rousseau</i> , 628 F. App'x 1022 (11th Cir. 2015)	36
<i>United States v. Schave</i> , No. CR 20-59 (ECT/BRT), 2020 WL 7133126	35
<i>United States v. Suellentrop</i> , 953 F.3d 1047 (8th Cir. 2020)	23
<i>United States v. Thomas</i> , 955 F.2d 207 (4th Cir. 1992).....	46
<i>United States v. Tillotson</i> , No. 2:08-CR-33, 2008 WL 5140773 (E.D. Tenn. Dec. 2, 2008).....	30, 31, 32, 33
<i>United States v. Vosburgh</i> , 602 F.3d 512 (3d Cir. 2010).....	22
<i>Zurcher v. Stanford Daily</i> , 436 U.S. 547 (1978)	30
STATUTES	
§ 18-6-403, C.R.S. (2015)	5

TABLE OF AUTHORITIES

PAGE

RULES

C.A.R. 53(a)(3)..... 44

Crim. P. 41(e) 10

OTHER AUTHORITIES

Reader’s Digest, *125 Funny Wi-Fi Names for a Hilarious Internet*

Connection 39

University of Colorado Denver, *Wireless Network and Connectivity*.... 41

INTRODUCTION

A detective obtained a facially valid search warrant for electronic devices found at a residential property associated with an internet account that had been used to download child pornography. When the detective arrived on the scene, he learned that Defendant Kevin Matthew Dhyne lived in a room in the basement and used the homeowner's internet account.

This case isn't about a "shoddy" police investigation; it's about the judgment call the detective had to make on the scene about the warrant's scope. The detective reasonably interpreted the warrant as authorizing him to search Dhyne's room, and the court of appeals agreed. The trial court, on the other hand, concluded the detective shouldn't have searched Dhyne's room but admitted the fruits of that search under the exclusionary rule's inevitable discovery exception. Under either rationale, Dhyne's conviction should be upheld.

STATEMENT OF THE FACTS AND THE CASE

I. The investigation

A detective received a tip from another law enforcement officer that a person was illegally downloading child pornography using an Internet Protocol (IP) address associated with a Comcast subscriber. (CF, pp 2, 373.) Through subpoenas to Comcast, the detective narrowed the internet activity to an account belonging to subscriber D.C. (CF, p 2, 373.) Any device that accessed the internet through D.C.'s account at that time would have been using that IP address. (TR 5/14/18, pp 4-6.)

The detective researched D.C.'s street address, checking with the county assessor's office and confirming that the residence was listed as a single-family home. (TR 5/14/18, p 8:8-19.) The detective also knew from prior law enforcement experience that D.C.'s adult son, B.C., lived on the property and was a registered sex offender. (TR 5/14/18, pp 7-8.)

The detective sought a warrant for electronic devices and other related evidence at D.C.'s property, which was described as: "House, garage and any outbuildings located at [REDACTED]"

Clear Creek County[,] Colorado.” (CF, p 118.) It contained a description of the house and the structure where B.C. lived. (CF, p 118.) A judge issued the search warrant. (TR 5/14/18, p 13:8-9.)

Upon arriving at the address to execute the warrant, the detective observed that the house appeared to be a single-family home with one marked address, one mailbox, and no other markings to indicate a multi-unit dwelling. (TR 5/14/18, p 13:8-24.) The detective saw Dhyne outside the house near a door, and Dhyne “told [him] that he was living in that room down there, down in the basement.” (TR 5/14/18, p 15:2-9.) The detective explained why he was present and asked Dhyne if he used the homeowner’s internet; Dhyne said he did. (TR 5/14/18, p 16:8-10.) The detective knew that Dhyne was facing charges for sexual assault on a child (of which he was later acquitted). (TR 5/14/18, pp 16:23, 17:3-6.)

The detective concluded that he was authorized to search “the whole property,” including Dhyne’s room in the basement of the house. (TR 5/14/18, pp 20-21.) The basement contained a refrigerator and stove and a small living and bedroom area. (TR 5/14/18, p 15:12-15.) The

detective seized Dhyne's computers, as well as devices from the rest of the property. (TR 5/14/18, pp 21:8-13; TR 2/26/20, pp 95-96; CF, p 373.)

Only one device seized—a laptop taken from Dhyne's room that Dhyne identified as his—contained sexually exploitative material. (TR 2/26/20, pp 17-18, 95-96.) Dhyne's laptop was password-protected and had a Torrent application on it, which is often used to download child pornography. (TR 2/26/20, pp 22-23, 33:5-25.)

The prosecution charged Dhyne with two counts of sexual exploitation of a child. (CF, pp 31-33.)

II. Trial court proceedings

Dhyne filed a motion to suppress, asserting that the warrant did not allow officers to search his basement room. (CF, pp 108-09.) The trial court held an evidentiary hearing, which included testimony from the detective and photos of the residence.

The court found the warrant facially valid because the detective had exercised diligence and had no reason to know that the single-family home contained a second unit when he applied for the warrant.

(CF, pp 147-48.) The court reasoned, however, that once the detective learned on the scene that Dhyne lived in a “separate dwelling unit,” the basement should not have been searched. (CF, p 148.)

The court then ruled that the inevitable discovery exception to the exclusionary rule applied. (CF, p 149.) The court concluded that regardless of the illegal search of Dhyne’s apartment, any competent law enforcement officer who knew child pornography was being downloaded to an IP address associated with the physical address of [REDACTED] would obtain a search warrant for the remainder of the house, and probable cause would have existed for that warrant. (CF, p 149.)

Dhyne opted for a bench trial. The parties stipulated that the laptop contained one video and more than twenty images that constituted “sexually exploitative material” under section 18-6-403, C.R.S. (CF, p 373.) Dhyne’s theory of defense was that the prosecution could not prove he knowingly possessed the images and that D.C. and

B.C. had access to his residence. (CF, pp 391-94.)¹

A forensic computer expert found 241 files on the laptop that appeared to be child pornography. (TR 2/26/20, p 81:19-22.) The expert testified that the video file had been accessed at least once. (TR 2/26/20, p 34:17-19.) The laptop also revealed searches the user had run for terms associated with child pornography. (TR 2/26/20, pp 37-38.) The expert concluded the presence of child pornography on the laptop was not an “anomaly” but a “concerted effort by the user to ... procure files” with names associated with child pornography, demonstrating “a definite user interest in these types of files.” (TR 2/26/20, pp 48:4-10, 81:15.)

The court found Dhyne guilty on both counts. (TR 6/2/20, p 3:1-8.) It sentenced him to ten years of sex offender intensive supervision probation. (CF, p 485.)

¹ The court denied Dhyne’s alternate suspect defense, but the parties still stipulated to admission of evidence from D.C.’s and B.C.’s interviews as well as Dhyne’s lease agreement. (TR 2/26/20, pp 11-12.)

III. The appeal

On appeal, Dhyne challenged the trial court's suppression ruling, its ruling precluding his alternate suspect defense, and the sufficiency of the evidence.

The division affirmed, finding the search of Dhyne's room did not violate his Fourth Amendment rights and declining to reach the inevitable discovery exception. The majority opinion reasoned that “[b]ecause police had information that the IP address linked to the subscriber's physical address (the basis for probable cause) was commonly used by Dhyne in his separate residence at that physical address, the search of Dhyne's apartment was authorized by the warrant, notwithstanding his separate unit.” *People v. Dhyne*, 2022 COA 122, ¶16.

Judge Richman specially concurred, agreeing with “the result the majority reaches and most of their rationale.” *Id.* at ¶36. He was persuaded by federal case law, however, that the more “appropriate legal lens through which to analyze the search in this case” is to

consider whether “the entire premises were suspect” rather than analogizing shared use of an IP address to common occupation of a physical premises. *Id.* at ¶¶36-50. Using that lens, he agreed with the majority that Dhyne’s Fourth Amendment rights were not violated. *Id.* at ¶50.

The division also found the evidence sufficient to support the conviction and that the trial court properly excluded the alternate suspect evidence. *Id.* at ¶¶21-34.

SUMMARY OF THE ARGUMENT

I. A warrant must describe with particularity the places to be searched and the things to be seized, and it must be supported by probable cause. Officers executing facially valid warrants often encounter situations in which they must make judgment calls about those places to be searched and things to be seized. If they act reasonably, no Fourth Amendment violation occurs.

When faced with an ambiguity about a multi-unit property, officers act reasonably by executing a warrant for an area not

specifically described in the warrant if (1) there is common occupancy or control or (2) the entire premises are suspect.

Here, the detective encountered an ambiguity about the place to be searched when he executed the facially valid warrant: Dhyne told him he lived in the basement and used the homeowner's internet. He searched Dhyne's room. The court of appeals' majority and special concurrence applied two different rationales—an analogy to common occupancy and the entire premises being suspect—to conclude that the search did not violate Dhyne's Fourth Amendment rights. Either rationale supports admission of the evidence, and cases from numerous other jurisdictions support their conclusion. This Court should affirm.

II. Alternatively, the trial court correctly applied the inevitable discovery exception to the exclusionary rule. Under the inevitable discovery exception, evidence initially discovered in an unconstitutional manner may be received if that same evidence inevitably would have been obtained by lawful means. Here, the information that made the discovery inevitable arose independent of any illegal search: the

detective learned before the search that Dhyne lived in the basement and used the homeowner's internet, and the detective also knew that Dhyne was then facing charges of sexual assault on a child. The inevitable discovery exception's use was appropriate here.

ARGUMENT

I. Law enforcement reasonably concluded that the warrant authorized a search of Dhyne's room.

A. Preservation and standard of review

A defendant can move to suppress evidence unlawfully seized under Crim. P. 41(e). The defendant, as the moving party, bears the burden of going forward, and if the defendant satisfies this burden, the prosecution must rebut the allegations. *People v. Morehead*, 2019 CO 48, ¶12.

The People agree that this Court's review of a trial court's suppression order presents a mixed question of fact and law. *People v. McKay*, 2021 CO 72, ¶4. This Court defers to the trial court's factual findings that are supported by competent evidence and reviews the legal effect of those facts de novo. *Id.*

The People agree, in part, with Dhyne's statement on preservation. Dhyne moved to suppress the evidence seized from his basement room. He preserved the argument that the search violated the Fourth Amendment because the detective's execution of the warrant was overbroad, and in the alternative, that the evidence was not admissible under the inevitable discovery exception. (CF, pp 114-15, 132-43; TR 5/14/18, pp 36-40; COA OB, pp 4-13.)

Dhyne abandoned any claim under the Colorado Constitution by failing to raise it in the court of appeals. (COA OB, pp 4-13.) *People v. Mershon*, 874 P.2d 1025, 1036 (Colo. 1994).²

Dhyne also makes new arguments that the detective did not attempt to determine, prior to obtaining the warrant, who used D.C.'s

² When this Court granted certiorari, it retained Dhyne's framing of the issues, including references to the Colorado Constitution. Even if the state constitutional issue were properly before this Court, however, Dhyne still does not develop an argument under the state constitution, reciting simply that its privacy protections are broader than under the U.S. Constitution. (OB, pp 12, 32.) This Court should address only the preserved and developed federal constitutional issue. *Mershon*, 874 P.2d at 1036.

internet and how it was configured, which he contends affects the probable cause analysis. (OB, pp 8, 16-19.) But he did not raise these arguments in the trial court or court of appeals. (CF, pp 132-43; COA OB, pp 8-13.)

In making these new arguments, he also repeatedly asserts a fact not in evidence: that B.C. had an open (not password-protected) router connected to D.C.'s password-protected router. (OB, pp 8, 16-19.) He cites to Dhyne's arrest affidavit for that fact, but the affidavit recounts that B.C. said it was open but was also uncertain and advised police "to ask his mother." (CF, p 7.) There was no evidence adduced about the home's routers at the suppression hearing or trial; the word "router" does not even appear in any transcript, motion, or appellate brief until Dhyne's Opening Brief in this Court—where it belatedly plays a prominent role.

This Court does not review arguments not raised in the court of appeals. *Mershon*, 874 P.2d at 1036.

B. Relevant law

1. Facial validity of a warrant

“The Fourth Amendment to the United States Constitution ... prohibit[s] the issuance of a search warrant except upon probable cause supported by oath or affirmation particularly describing the place to be searched and the things to be seized.” *People v. Cooper*, 2016 CO 73, ¶8.

Probable cause exists when an affidavit for a search warrant alleges sufficient facts to warrant a person of reasonable caution to believe that contraband or evidence of criminal activity is located at the place to be searched. *Id.* at ¶9. “[T]he scope of a lawful search is defined by the object of the search and the places in which there is probable cause to believe that it may be found.” *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (citation omitted).

A warrant’s scope is constrained by the Fourth Amendment’s requirements that the warrant be sufficiently particular and not overbroad. “By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement

ensures that the search ... will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.”

Garrison, 480 U.S. at 84.

A search warrant for a multi-unit structure is sufficiently particular if it “sufficiently describe[s] the apartment or sub[-]unit to be searched, either by number or other designation, or by the name of the tenant or occupant.” *People v. Avery*, 173 Colo. 315, 319, 478 P.2d 310, 312 (1970).

2. Reasonableness of a warrant’s execution

“A warrant that seems unambiguous to a magistrate in the confines of the courthouse may not be so clear during the execution of the search, as officers encounter new information not available when they applied for the warrant.” *United States v. Aljabari*, 626 F.3d 940, 947 (7th Cir. 2010).

“Warrants with ... errors or ambiguities are not new.” *Muhammad v. Pearson*, 900 F.3d 898, 904 (7th Cir. 2018). “[A]t some point during any search the executing officer must exercise his or her

judgment in applying the language of the warrant to the premises to be searched.” *People v. Roccaforte*, 919 P.2d 799, 803 (Colo. 1996) Thus, “the validity of a warrant” on its face and the “reasonableness of the manner in which it was executed” are “two separate constitutional issues. *Garrison*, 480 U.S. at 84. “[A]n executing officer must interpret a warrant’s terms reasonably, but the officer need not give them the narrowest possible reasonable interpretation.” *Aljabari*, 626 F.3d at 947.

The need to exercise judgment while executing a warrant is especially common in multi-unit residences where “officers seeking search warrants cannot [always] obtain accurate information (especially about the interiors of multi-unit buildings), at least not without alerting the targets of the investigation.” *Muhammad*, 900 F.3d at 904.

The seminal U.S. Supreme Court case that addresses a warrant’s execution on a previously unknown multi-unit structure is *Garrison*. In that case, officers found contraband in the apartment specified in their warrant but belatedly realized the apartment they were searching had

been divided into two separate units. *Garrison*, 480 U.S. at 81. They stopped the search, but the contraband had already been found in the unit not associated with the suspect. *Id.*

The Court first concluded the warrant was facially valid and held that the officers' later discovery of facts demonstrating the warrant was too broad did not "retroactively invalidate [it]." *Id.* at 85. Then the Court analyzed the warrant's execution, concluding the defendant's Fourth Amendment rights were not violated: "the officers' conduct was consistent with a reasonable effort to ascertain and identify the place intended to be searched within the meaning of the Fourth Amendment." *Id.* at 88.

Prior to *Garrison*, this Court had addressed a similar situation in which officers executing a search warrant were initially unaware that a home had multiple units in *People v. Lucero*, 174 Colo. 278, 280, 483 P.2d 968, 970 (1971). When the officers "entered the premises, it became apparent that the house was divided into two living quarters on the main floor, with a third on the second floor." *Id.* at 280. This Court

concluded that no Fourth Amendment violation occurred because (1) the officers did not know the home was a multi-unit structure until they entered it, and (2) they cabined their search to the area for which there was probable cause. *Id.* at 280-81.

Before and since *Garrison*, this Court has also addressed situations in which there is common occupancy or control of a premises by multiple people. If persons share a living space, and they have areas of common use and the “ability to access” other private areas (like bedrooms), then the police can search those areas “to protect against the possibility” that the items to be seized are hidden in those areas. *People v. Webb*, 2014 CO 36, ¶ 12; *see also People v. Ward*, 181 Colo. 246, 249, 508 P.2d 1257, 1259 (1973); *People v. Martinez*, 165 P.3d 907, 912 (Colo. App. 2007).

Similarly, courts in other jurisdictions have identified three recurring situations in which the search of a multi-unit structure does not violate a person’s Fourth Amendment rights. “The general rule voiding the warrant for an undisclosed multiunit structure ... does not

apply [1] if the defendant was in control of the whole premises or they were occupied in common, [2] if the entire premises were suspect, or [3] if the multi[-]unit character of the premises was not known to the officers [when the search was performed].” *United States v. Gilman*, 684 F.2d 616, 618 (9th Cir. 1982) (citation omitted; emphasis added).³

The first situation, shared occupancy, arose in this Court’s *Webb* and *Ward* opinions, as well as the court of appeals’ opinion in *Martinez*. This Court has not yet addressed the second situation, where the entire premises are suspect. And the third, a search conducted before the officers realized there were separate premises, arose in this Court’s *Lucero* opinion.

³ See also *United States v. Kaplan*, 526 F. Appx. 208, 215, n.6 (3d Cir. 2013); *United States v. Johnson*, 26 F.3d 669, 694 (7th Cir. 1994); *Booth v. Antill*, 849 F.2d 604 (4th Cir. 1988); *Ramirez v. Webb*, 835 F.2d 1153, 1157 (6th Cir. 1987); *United States v. Butler*, 793 F.2d 951, 952 (8th Cir. 1986); *Peters v. State*, 120 A.3d 839, 861, n.11 (Md. Ct. Spec. App. 2015); *State v. Hawkins*, 201 P.3d 239, 244 (Ore. Ct. App. 2009); *State v. Teague*, 469 So. 2d 1310, 1316 (Ala. Crim. App. 1985); *State v. Patmon*, 604 P.2d 82, 84 (Kan. Ct. App. 1979).

C. Analysis

The detective obtained a facially valid search warrant here because the warrant described with particularity the places to be searched and the things to be seized, and it was supported by probable cause.

Then the detective arrived on the scene to execute the warrant and faced an ambiguity: did the warrant allow him to search Dhyne's previously undisclosed basement room? He concluded that it did. If his conclusion was reasonable, then his search did not violate Dhyne's Fourth Amendment rights.

The court of appeals concluded the evidence was admissible based on two slightly different rationales. The majority opinion relied on an analogy to the common occupancy or control cases, like *Webb*, *Ward*, and *Martinez* where probable cause exists as to one area but common access or control allows for a search of the rest of the premises. Judge Richman's special concurrence relied on a related ground accepted by other courts but not yet addressed by this Court, the entire premises

being suspect. Either rationale supports admitting the evidence here.

1. The warrant was facially valid.

Despite Dhyne’s remarks about a “shoddy” police investigation, he focuses on the warrant’s execution rather than arguing it was facially invalid. (OB, pp 11-22.) This focus matters because, as *Garrison* explains, the warrant’s facial validity and the lawfulness of the warrant’s execution are “two separate constitutional issues.” *Garrison*, 480 U.S. at 84.

The detective obtained a search warrant specifying the place to be searched as: “House, garage and any outbuildings located at [REDACTED] [REDACTED] Clear Creek County[,] Colorado.” It also contained a description of the house and B.C.’s living space. (CF, p 118.)

The affidavit explained that child pornography had been downloaded using an IP address that Comcast identified as belonging to its subscriber D.C., and that B.C., a registered sex offender, also lived at that address in a separate structure. (CF, pp 119-22.) The affidavit also

explained the steps the detective took to confirm that D.C. lived at the house and that it was a single-family home. (CF, pp 119-22.)

The trial court found the warrant facially valid. It concluded the detective's investigation into the residence's character as a single-family home and confirmation of the homeowner as D.C. through the assessor's office was "sufficiently diligent." (CF, p 148.) It also found that visual observation of the home would *not* have disclosed the existence of a separate basement unit, which was not separately marked or visible from the street. (CF, p 148.)

The homeowner's address and identity matched the Comcast subscriber's address and identity, and her IP address had been used to download the sexually exploitative material. (CF, pp 119-22.) Dhyne claims "the record is absent of any attempts by [the] investigators to subpoena the Comcast records." (OB, pp 17-18.) But that isn't true—the detective described two subpoenas to Comcast and the information he received in return in the search warrant affidavit, which was admitted

into evidence at the suppression hearing. (CF pp 119-22; TR 5/14/18, pp 8-9.)⁴

Courts routinely find probable cause when an investigation connects a particular user's IP address to their residential address, as the detective did here, linking the IP address to D.C.'s internet account and verifying that she lived at the residential address. *See, e.g., United States v. Vosburgh*, 602 F.3d 512, 526 (3d Cir. 2010) (“[S]everal Courts of Appeals have held that evidence that the user of a computer employing a particular IP address possessed or transmitted child pornography can support a search warrant for the physical premises linked to that IP address.”).

In assessing facial validity of a warrant, “the central question for the reviewing court is not whether it would have found probable cause in the first place, but whether the magistrate had a substantial basis for issuing the search warrant.” *McKay*, ¶10. The magistrate had a

⁴ The parties also stipulated at trial that Comcast had provided documents. (TR 2/26/20, p 5:4-14.)

substantial basis to issue the search warrant here. And the trial court's findings in reviewing the warrant are supported by the record, so they must be given deference on appeal. (TR 5/14/28, pp 3-32; People's Ex. B1-B3.) *McKay*, ¶4.

2. The detective's execution of the search warrant was lawful.

The crux of this case is whether the officer's execution of the warrant violated Dhyne's Fourth Amendment rights. "[T]he question is whether the officer[] *reasonably believed* that the warrant authorized the search, even if [his] interpretation was mistaken." *United States v. Suellentrop*, 953 F.3d 1047, 1050 (8th Cir. 2020) (emphasis in original). The constitution requires that the factual determinations made "by ... the police officer executing a warrant ... is not that [he] always be correct, but that [he] always be reasonable." *Illinois v. Rodriguez*, 497 U.S. 177, 185 (1990).

Here, the detective learned that Dhyne lived in the basement of the home and used D.C.'s internet account before he executed the warrant. (TR 5/14/18, p 15:2-9, 16:8-10.) The detective concluded that

the warrant allowed him to search the basement because, in his view, the search warrant covered “the whole property at [REDACTED]” (TR 5/14/18, pp 20-21.) He searched Dhyne’s room in the basement, as well as the rest of the property. (TR 5/14/18, pp 21:8-13; CF, p 373.)

The trial court reasoned, citing *Avery*, that the warrant did not authorize the detective to search Dhyne’s unit once the detective learned from Dhyne that he had a “separate dwelling.” (CF, p 148.) True, that communication alerted the detective to the possibility of a multi-unit residence. But Dhyne didn’t use the term “separate dwelling” and the court didn’t make that finding (at least not explicitly). The detective just testified at the suppression hearing that Dhyne said he lived in “that room down there, down in the basement”; regardless, Dhyne’s characterization of his living space isn’t controlling. *See Martinez*, 165 P.3d at 912 (“[T]he police were not obligated to believe the statements of defendant’s mother describing her limited access to defendant’s bedroom.”). Yet by relying on *Avery* and Dhyne’s statement,

the trial court failed to complete its analysis before turning to the inevitable discovery exception.⁵

The court of appeals correctly went on to consider that other recognized grounds can justify the search of a unit in a multi-unit residence during execution of the warrant. The majority adopted the reasoning from *Martinez* and concluded that D.C.’s internet account, which was the basis for probable cause to search the residence, was shared in common with Dhyne and provided grounds to search his residence. *Dhyne*, ¶¶15-20. Judge Richman, on the other hand, concluded the entire premises were suspect. *Id.* at ¶¶36-50. Either rationale supports the conclusion that the detective acted reasonably.

The majority’s opinion, which reasoned that Dhyne’s room could be searched because he shared D.C.’s internet account, is not as odd as

⁵ The trial court also didn’t make any findings about D.C.’s and B.C.’s “ability to access” Dhyne’s room, which could also have been grounds to search it. *See Webb*, ¶9. Dhyne attempted to adduce evidence of their ability to access his room (and his laptop) at trial to disprove that he committed the offense. (TR 2/26/20, pp 8-9, 117-18.) By that point, the evidence had been ruled admissible, so the prosecution did not have any reason to pursue this alternate line of admissibility.

Dhyne makes it out to be. The majority discussed the common occupancy exception and concluded that when Dhyne told the detective that he shared D.C.'s IP address, "the police had reason to believe that the area to be searched—the parts of the physical address from which the IP address could be accessed"—fell within the warrant's scope.

Dhyne, ¶¶15-20.

In common occupancy cases, the basis for concluding that the warrant was executed appropriately is the multiple occupants' use of parts of the premises without restriction, so the police can search for the items identified in the warrant anywhere those items could reasonably be located. *Webb*, ¶¶12-17 (concluding a warrant authorized the officers' search for methamphetamine in the bedroom and inside the purse of a person whose actions did not form part of the warrant's probable cause).

Dhyne's internet access is conceptually similar; the homeowner's internet account was shared with him, so the detective could search any area of the premises from which the internet could be accessed. The

majority's analogy is appropriate, even if not a precise fit. *In re Warrant Application*, No. 22 M 00595, 2023 WL 1878636, at *21 (N.D. Ill. Feb. 1, 2023) (“Fourth Amendment doctrines rooted in Colonial Era grievances do not always map neatly onto 21st century ... technologies.”).

While other courts may not have expressly drawn the analogy to shared occupancy drawn by the majority, courts have reasoned that a particular search was authorized by a warrant due to the presence of shared internet access or, conversely, that a search wasn't reasonable in the absence of shared internet access. *See, e.g. Jeffers v. Commonwealth*, 743 S.E.2d 289, 291 (Va. Ct. App. 2013), (noting “computer router inside the trailer supplied Internet access to the barn” where the defendant resided); *United States v. Huntoon*, No. R1600046001TUCDCBDTF, 2018 WL 1755788, at *5 (D. Ariz. Apr. 12, 2018) (noting that the IP address associated with the residence was shared by the fifth wheel trailer and holding that the search of the trailer was authorized); *Commonwealth v. Molina*, 71 N.E.3d 117, 126-28 (Mass. App. Ct. 2017) (even though five people lived in a residence

where the internet subscriber’s IP address had been used to download child pornography, the search of defendant’s unlocked bedroom was proper because “computer devices using the monitored IP address [could] be anywhere in the apartment”); *cf. Doe v. Olson*, 691 F. App’x 272, 274-75 (8th Cir. 2017) (finding officers who obtained a search warrant were entitled to qualified immunity for searching a basement sub-unit after learning that “all of the occupants ... could wirelessly access the residence’s internet service”); *People v. Nguyen*, 12 Cal. App. 5th 574 (2017) (the search of a residence on the property behind the main residence wasn’t proper because it wasn’t identified in the warrant and there was *no evidence of shared internet*).

On the other hand, Judge Richman’s special concurrence adopted the “entire premises are suspect” reasoning. Dhyne calls this analysis “untested” and urges this Court not to adopt it. (OB, p 20.) Although the reasoning hasn’t been adopted in Colorado, it is not untested, having been accepted in other jurisdictions for decades. *See infra*, n.3. And the

concept is not novel: it just means probable cause extended to each unit in the premises.

Dhyne's basement room was within a structure described in the warrant. The warrant didn't *exclude* the basement, and it *included* all the other structures on the property, even multiple residences. By contrast, in *United States v. Ayala*, 646 F. Supp. 3d 1191, 1196-97 (N.D. Cal 2022), a warrant authorized a search for evidence of child pornography within a red and green structure at an address, but officers searched a yellow structure that was also located at that address. The court held the warrant could not reasonably be read to authorize the officers' search of the yellow structure because it didn't fit the description in the warrant. *Id.* No such limitation appeared in the warrant here, and Dhyne doesn't dispute the accuracy of the description contained in the warrant.

And the warrant's failure to identify Dhyne by name does not undercut the reasonableness of the detective's interpretation either. "Search warrants are not directed at persons; they authorize the search

of ‘place[s]’ and the seizure of ‘things,’ and as a constitutional matter they need not even name the person from whom the things will be seized.” *Zurcher v. Stanford Daily*, 436 U.S. 547, 555 (1978) (alteration in original).

The detective’s affidavit identified that B.C. “would be a possible suspect.” (CF, p 122.) But it could not be more specific under the circumstances because the detective did not know who used the homeowner’s internet account to download the child pornography—and the court-approved warrant didn’t limit the search to just B.C.’s living space or his devices. “As far as [law enforcement] knew, *any* of the occupants of [the address]—or all of them, for that matter—could have used the computer to send and receive child pornography.” *United States v. Tillotson*, No. 2:08-CR-33, 2008 WL 5140773 (E.D. Tenn. Dec. 2, 2008) (concluding that the search warrant based on an IP address “was as ‘tailored’ as it could be under the circumstances.”); *see also Zurcher*, 436 U.S. at 561 (“[S]earch warrants are often employed early

in an investigation, perhaps before the identity of any likely criminal and certainly before all the perpetrators are or could be known.”).

In favoring the “legal lens” that the entire premises were suspect, Judge Richman found two federal district court cases persuasive:

United States v. Axelrod, No. WDQ-10-0279, 2011 WL 1740542 (D. Md. May 3, 2011) and *Tillotson*, 2008 WL 5140773. *Dhyne*, ¶¶36, 43-49.

In *Axelrod*, officers obtained a search warrant for what they believed was a single-family home where an IP address associated with the physical address had been used to download child pornography. 2011 WL 1740542, *1. But the single-family home included a separate in-law suite where the defendant lived; at the suppression hearing, a factual dispute arose as to whether the officers learned the in-law suite was a separate residence before or after they searched it. *Id.* at *4-5. The district court found no Fourth Amendment violation, even if the officers had been told the defendant lived in the in-law suite before they searched it. *Id.* at *5. The court reasoned that “the warrant could reasonably be interpreted as providing probable cause to search all of

[the residential address]—the entire premises were suspect because the internet connection was open and anyone in the residence could access it.” *Id.* at *5 (internal citation omitted).

Similarly, in *Tillotson*, officers obtained a search warrant for a residence at a street address where an IP address had been used to download child pornography. 2008 WL 5140773, *7. The defendant argued that the search warrant was executed in an overbroad manner because the home was a multi-family residence, yet the officers had searched the entire residence. The district court disagreed: “As far as the United States knew, *any* of the occupants of [the address]—or all of them, for that matter—could have used the computer to send and receive child pornography.” *Id.*

Dhyne’s attempts to distinguish *Axelrod* and *Tillotson* on the facts should be rejected. He incorrectly asserts that *Axelrod* is distinguishable because officers didn’t know about the in-law suite until after the search, but that fact was disputed at the suppression hearing, and the court made an alternative holding that the search was proper

even if officers knew in advance because the entire premises were suspect. *Axelrod*, 2011 WL 1740542, *5. As for *Tillotson*, Dhyne asserts that probable cause was based on “a single computer used for downloading and sending child pornography” (OB, p 21), but the court didn’t interpret the warrant as limiting the search to the location of that single computer. 2008 WL 5140773, *7. It explicitly held that the warrant “authorized [the officer] to search throughout the *entire* house” because the officer didn’t know “where the *computer (or computers)* and other electronic storage devices might be located.” *Id.* (emphasis added).

Unsurprisingly, Fourth Amendment cases often turn on details that are unlikely to be precisely mirrored in other cases: what the warrants say, the probable cause that supported them, the layout of the premises, the people that lived therein, the facts officers learned on the scene, and when they learned them. This variety in factual scenarios is why the U.S. Supreme Court cautioned courts to “allow some latitude for honest mistakes that are made by officers” executing warrants when those mistakes are objectively reasonable. *Garrison*, 480 U.S. at 87 &

n.11. In the Fourth Amendment context, “there is ‘no valid substitute for careful case-by-case evaluation of reasonableness.’” *United States v. Lewis*, 62 F.4th 733, 743 (2d Cir. 2023) (quoting *Missouri v. McNeely*, 569 U.S. 141, 158 (2013)).

Despite any differences between *Axelrod* and *Tillotson* and this case, they still broadly support that the detective acted reasonably here. And courts in other jurisdictions have found searches authorized under similar circumstances.

For example, in *Jeffers*, 743 S.E.2d at 290, officers determined that an IP address had been used to download child pornography and obtained a warrant to search the internet subscriber’s property, which consisted of a residential trailer and a barn. When officers arrived to execute the warrant, they learned from the homeowner that someone lived in the barn and used her internet account; officers searched the barn anyway. *Id.* at 290-91. The defendant argued that “once the officers discovered that [he] lived in the barn, they could not search the barn because it was no longer within the scope of the warrant.” *Id.* at

291. The Virginia Court of Appeals disagreed, concluding that officers could reasonably interpret the warrant as authorizing search of the barn even after discovering that someone lived there because “police had traced child pornography to this address, but did not know in which of the [buildings] the illegal transactions [were] taking place.” *Id.* at 292 (alterations in original, citation omitted).

In *United States v. Houck*, 888 F.3d 957, 958 (8th Cir. 2018), police determined that an IP address had been used to download child pornography and obtained a warrant to search the internet subscriber’s residence and any vehicles on the property. When officers executed the search warrant, they searched a “fifth wheel” trailer in the driveway, which was not attached to any other vehicle and was connected to electrical and water lines. The defendant argued that the warrant did not authorize the search because the fifth wheel was his separate residence. The Eighth Circuit disagreed, concluding “it was not objectively unreasonable for the officers to believe that the [fifth wheel] was a vehicle within the scope of the warrant.” *Id.*; see also *United*

States v. Schave, No. CR 20-59 (ECT/BRT), 2020 WL 7133126 (D. Minn. Aug. 26, 2020 (a warrant authorizing a search of a residence where an IP address had downloaded child pornography was not overbroad, reasoning that “even though the officers learned that more men lived in the home than they originally knew about, there was still a fair probability that the illegal transmissions were made within the home”); *cf. United States v. Rousseau*, 628 F. App’x 1022, 1026-27 (11th Cir. 2015) (a warrant authorizing a search anywhere in a fire station was not overbroad because “agents [who] were investigating the downloading and sharing of child pornography using an IP address registered to the Station ... did not know which or how many Station employees might be involved in the activity”).

As in *Garrison*, the detective’s “conduct was consistent with a reasonable effort to ascertain and identify the place intended to be searched within the meaning of the Fourth Amendment.” *Garrison*, 480 U.S. at 87-88 & n.11 (“allow[ing] some latitude for honest mistakes that are made by officers in the dangerous and difficult process of making

arrests and executing search warrants,” as long as the officer’s actions are objectively reasonable). Here, the detective’s belief that Dhyne’s basement room fell within the scope of the warrant was objectively reasonable.

3. Dhyne’s concerns about probable cause from shared internet are not preserved or pertinent to this case.

As previously noted, Dhyne didn’t preserve the arguments he now makes about the lack of probable cause due to inadequate investigation of the internet account and its users, and he argues facts not in evidence about D.C.’s and B.C.’s routers and their password-protection or lack thereof.

The facts in evidence consist of the detective’s suppression hearing testimony and initial warrant affidavit where the detective described the process undertaken (1) to identify the Comcast subscriber whose IP address had been used to download the files, (2) to verify that the Comcast subscriber listed was also the person who owned and lived in

the home, and (3) to confirm, to the extent possible, that the residence was a single-family home. (TR 5/14/18, pp 8-9; CF, pp 119-22.)

With the benefit of hindsight, Dhyne faults the detective for not determining who was using the internet. He doesn't explain how law enforcement could do that. Indeed, Amici Curiae Professors of Law & Engineering explain that "a subpoena directed at an [internet service provider] can only identify the name and address of the subscriber whose internet connection may have been used in the commission of a crime—but not necessarily the owner of the device, or more importantly the person who used the device for the activity in question." (Amicus Br., pp 12-13 (emphasis deleted).)

Likewise, Dhyne faults the detective for not investigating the routers' configuration and whether they were open or password-protected. He doesn't explain how an investigator could learn that information about a router located *inside* a person's home. Even if an investigator physically surveilling a property located an open wireless signal, users can name their routers anything, like "No More Mr. WiFi"

or “Wi-Fi Fo Fum,”⁶ which wouldn’t tell the investigator from which house the signal originated (unless the house was isolated).

As discussed in Argument Section I.C.1, courts find probable cause when an IP address connected to internet subscriber’s account has been used for illegal activity, and the subscriber’s account is verified to have a connection with the residential address where the search will take place. That verification occurred here, and then Dhyne further provided the detective with the link connecting Dhyne to the IP address when he told the detective that he lived there and used the homeowner’s internet account.

Amici discuss concerns specific to wireless internet, which can be open to the public. They cite to *Nguyen*, in which officers obtained a search warrant for a single-family residence associated with an IP address that had downloaded child pornography. *Nguyen*, 12 Cal. App. 5th at 578. Officers searched that residence as well as a “plainly ...

⁶ Reader’s Digest, *125 Funny Wi-Fi Names for a Hilarious Internet Connection*, <https://www.rd.com/article/funny-wi-fi-network-names/> (last visited January 28, 2024).

separate residence” behind it. *Id.* The court rejected the government’s contention that it could search the rear residence because the entire premises were suspect. *Id.* at 584. The court noted that the government presented no evidence of shared network access or even that the front residence used a wireless router. *Id.* at 587. It held that “[p]robable cause requires some additional information connecting a defendant’s residence to criminal activity other than merely being *in range* of a suspect wireless signal.” *Id.* at 585 (emphasis added).

But *Nguyen* doesn’t undercut the analysis here because Dhyne wasn’t merely in range of a possible wireless signal; he told the detective, before the search, that he used D.C.’s internet account on his laptop from the previously undisclosed basement room of the single-family home described in the warrant. On the basis of that information, the detective reasonably concluded that Dhyne’s room was within the scope of the warrant.

Dhyne also raises concerns about searches of “all dormitory rooms in one residence hall.” (OB, p 18.) But this concern is misplaced. Courts

must already apply a totality of the circumstances analysis to assessing probable cause. *See Cooper*, ¶9. Different technologies and different locales would affect that probable cause analysis in different ways. For example, students in a university residence hall are unlikely to share a single IP address like residents of a home sharing a residential internet account; even if they did, students usually access university computing resources with their university usernames and passwords, which would provide police with different, more user-specific, information than was accessible in this case when the detective applied for the warrant.⁷

Dhyne does not explain, nor could he, why a magistrate would authorize a warrant whose affidavit failed to address multiple users in a dormitory residence, much less how an executing officer could reasonably conclude that a warrant framed in terms of a single

⁷ *See, e.g.*, University of Colorado Denver, Wireless Network and Connectivity (describing how to access campus wireless internet with a university username and password), <https://www.ucdenver.edu/offices/office-of-information-technology/get-help/technology-troubleshooting/wireless-and-connectivity> (last visited January 28, 2024).

premises could justify searching devices in every room in a university residence hall.

Regardless, a search warrant cannot authorize a “general search” unsupported by probable cause, and the division’s analysis doesn’t invite that. “[C]areful case-by-case assessment” is appropriate here, as in most Fourth Amendment contexts. *McNeely*, 569 U.S. at 152.

Amici list factors that a court might consider in assessing probable cause and particularity for a search warrant under circumstances like these, such as “[t]he number of people and devices accessing the internet through a given IP address” and “[w]hether the internet connections at issue are wired or wireless.” (Amicus Br., p 21.) The People don’t disagree that some of the factors could be pertinent in some situations—on the other hand, some of the factors can’t be determined before obtaining a search warrant no matter how thorough the investigation. A list of technology-dependent factors will not help courts answer the key question: would a person of reasonable caution believe

that contraband or evidence of criminal activity is located at the place to be searched? *Cooper*, ¶9.

The showing here was sufficient for a residential internet account connected to the homeowner's residence where Dhyne admitted to using that internet account from a location within the home that the detective reasonably believed was authorized to be searched by the warrant.

This Court should affirm.

II. Alternatively, the trial court properly applied the inevitable discovery exception to the exclusionary rule.

A. Preservation and standard of review

As described in Argument Section I.A, the inevitable discovery exception issue is generally preserved.

Again, Dhyne abandoned any claim under the Colorado Constitution by failing to raise it in the court of appeals. (COA OB, pp 4-13.) And again, Dhyne makes new arguments regarding the routers based on facts that are not in evidence. *Infra*, p 12.

Dhyne also advances a new argument that this Court should adopt stricter requirements for applying the inevitable discovery

doctrine under the Colorado Constitution because its privacy protections are broader than the Fourth Amendment's (OB, pp 30-34), which he did not assert in the trial court or court of appeals. (CF, p 141; COA OB, pp 12-13.) In addition, the Court did not grant certiorari on this issue; rather, the second certiorari question asked whether the trial court violated Dhyne's federal and state constitutional rights by "[finding] that the inevitable discovery exception applied to the search of the petitioner's residence." The adoption of a new standard is not a "subsidiary issue clearly comprised therein," (C.A.R. 53(a)(3)), and this Court does not address issues not included in the order granting certiorari. *Id.*; see also *State v. Nieto*, 993 P.2d 493, 505 (Colo. 2000).

For the preserved issue, as in Argument Section I, this Court defers to the trial court's factual findings that are supported by competent evidence and reviews the legal effect of those facts de novo. *McKay*, ¶4.

B. Relevant law

Evidence derived from an unconstitutional search must be

excluded at trial unless an exception to the exclusionary rule applies.

People v. Tallent, 2021 CO 68, ¶14. “Because the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence, to warrant its application, law enforcement conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.” *Casillas v. People*, 2018 CO 78M, ¶22.

Accordingly, Courts have recognized various exceptions to the exclusionary rule, including the inevitable discovery exception. “Exclusion of physical evidence that would inevitably have been discovered adds nothing to either the integrity or fairness of a criminal trial.” *Nix v. Williams*, 467 U.S. 431, 446 (1984). Under the inevitable discovery exception, evidence initially discovered in an unconstitutional manner may be received if that same evidence inevitably would have been obtained by lawful means. *People v. Syrie*, 101 P.3d 219, 222. (Colo. 2004). “The fact that makes discovery of the evidence inevitable

must ‘arise from circumstances other than those disclosed by the unlawful search itself’ because otherwise the inevitable discovery exception will swallow the exclusionary rule.” *People v. Burolo*, 848 P.2d 958, 962 (Colo. 1993) (quoting *United States v. Thomas*, 955 F.2d 207, 211 (4th Cir. 1992)); *see also People v. Fields*, 2018 CO 2, ¶16 (The inevitable discovery must “aris[e] from circumstances other than those disclosed by the unlawful search itself.”). The prosecution bears the burden of proof by a preponderance of the evidence. *Nix*, 467 U.S. at 444.

C. Analysis

1. Discovery of the evidence was inevitable.

Assuming for purposes of this argument that the detective illegally entered Dhyne’s room, the trial court properly concluded that the evidence seized was admissible under the inevitable discovery exception.

The trial court found the People had carried their burden of proof because the detective had evidence that an IP address associated with

D.C.'s internet account had been used to download child pornography, and the detective knew that Dhyne was using that IP address too. (CF, p 149.) If the detective hadn't interpreted the search warrant as including Dhyne's room, the trial court "ha[d] no doubt" the detective would have obtained a search warrant for Dhyne's room, which would have been supported by probable cause. (CF, p 149.)

The trial court cited to *United States v. Mejia*, No. 08 CR 1019, 2012 WL 4434367, at *4 (N.D. Ill. Sept. 24, 2012), in which a federal district court applied the inevitable discovery exception under circumstances similar to this case. In *Mejia*, a detective had obtained and executed a search warrant based upon an IP address used to download child pornography, but the officer's investigation hadn't uncovered that the residence had two units. The court concluded that it couldn't tell from the defendant's motion whether the officer had exercised due diligence in investigating the residence, but rather than holding a suppression hearing, the court decided to first address the inevitable discovery exception. It concluded that a "warrant would

undoubtedly have been issued” based on the information already known to the officer, so “the government has met its burden to establish by a preponderance of the evidence that the information [the defendant] seeks to suppress inevitably would have been discovered by lawful means.” *Id.* at *4-5.⁸

Finding *Mejia* persuasive authority, the trial court applied the inevitable discovery exception here. The trial court reached the right conclusion. As required by *Burolo*, the information here that makes the discovery inevitable—the detective learning that Dhyne, whom he knew was then facing sexual assault on a child charges (and therefore might have an interest in viewing sexually exploitative material), was living in the home and using D.C.’s internet—arose from circumstances other than those disclosed by the unlawful search itself. And although the detective seized Dhyne’s laptops in this search, they were examined later by a forensic computer expert, so the search itself didn’t

⁸ The court also declined to address the arguments made about the reasonableness of the warrant’s execution under *Garrison* due to its alternative holding. *Id.* at *3 & n.3.

immediately reveal any evidence of a crime that might have been used to support a belated warrant. (TR 5/14/18, p 21:3-18.) This isn't a situation where an officer illegally entered a premises, saw contraband, and then claimed he would have found it anyway. *See People v. Diaz*, 53 P.3d 1171, 1176 (Colo. 2002) (“[A] valid search warrant nearly always can be obtained after the search has occurred....”).

“As long as the evidence discovered during [the] illegal search would have been discovered during a later legal search[,] and the second search inevitably would have occurred in the absence of the first, then the evidence may be admitted.” *United States v. Cooper*, 24 F.4th 1086, 1091 (6th Cir. 2022) (alterations in original, citation omitted). The purpose of the inevitable discovery exception is to “properly balance” “the interest of society in deterring unlawful police conduct and the public interest in having juries receive all probative evidence of a crime ... by putting the police in the same, not a worse, position that they would have been in if no police error or misconduct had occurred.” *Nix*,

467 U.S. at 432-33. Applying the exception here achieved that balance and put the police in the same position as if the error had not occurred.

Dhyne argues that the detective didn't sufficiently investigate the home's router configuration or whether its "router was his sole and exclusive avenue to access the internet." (OB, p 28.) He doesn't explain how the detective would have determined that without entering his residence or why it would matter when he admitted that he used the account that downloaded child pornography. And a judge had already approved the search warrant for the rest of D.C.'s property based on the same sort of information the detective learned about Dhyne on the scene prior to searching his room, so there is no doubt that the warrant would have been approved.

2. This Court should not adopt a different formulation of the inevitable discovery exception.

This issue is neither preserved nor fairly comprised within the certiorari issues, and this Court should not consider it.

Dhyne argues that the current inevitable discovery standard is too lax and urges this Court to follow *Rodriguez v. State*, 187 So. 3d 841 (Fla. 2015). He contends that following this case would “reaffirm the principle that the protections from unreasonable searches and seizures under the [state constitution] are greater than those afforded under the Fourth Amendment.” (OB, p 32.)

In *Rodriguez*, the Florida Supreme Court held that the inevitable discovery exception “can only apply if [police officers] actually were in pursuit” of a warrant at the time of the illegal search. *Id.* at 849. Florida appears to be the only jurisdiction to have adopted this requirement, and at least one other state supreme court explicitly rejected it. Citing *Rodriguez*, the Utah Supreme Court “decline[d] to adopt such a bright-line rule” because there could be other instances where evidence would have been lawfully discovered through other means. *Brierley v. City*, 390 P.3d 269, 276, n.6 (Utah 2016).

Some jurisdictions, like the Tenth Circuit, consider multiple factors in “assessing warrantless search situations,” but still retain the

flexibility to conduct a case-by-case analysis. “Numerous police actions are judged based on fact-intensive, totality of the circumstances analyses rather than according to categorical rules, including in situations that are more likely to require police officers to make difficult split-second judgments.” *McNeely*, 569 U.S. at 158.

The Tenth Circuit considers: (1) the extent to which the warrant process has been completed at the time those seeking the warrant learn of the search; (2) the strength of the showing of probable cause at the time the search occurred; (3) whether a warrant ultimately was obtained, albeit after the illegal entry; and (4) evidence that law enforcement agents “jumped the gun” because they lacked confidence in their showing of probable cause and wanted to force the issue by creating a *fait accompli*. *United States v. Cunningham*, 413 F.3d 1199, 1203-04 (10th Cir. 2005).

Dhyne relied on these factors in the court of appeals (COA OB, pp 12-13) but now urges *Rodriguez* instead; of course, the detective here

did not actually pursue a separate warrant for Dhyne’s room, so the analysis would end there under *Rodriguez*.

The Tenth Circuit factors support the trial court’s decision to apply the inevitable discovery rule. The detective received a warrant for the rest of the property, which he believed covered Dhyne’s room too. The probable cause showing was strong because Dhyne admitted to sharing the internet account that had been used to download child pornography, and Dhyne was then facing charges for sexual assault on a child. No warrant was ultimately obtained, even after the search. But there is no indication the detective doubted that probable cause existed and was creating a *fait accompli* (for instance, by trying to manufacture exigent circumstances)—he simply believed the warrant he already had authorized the search.

“Because the exclusionary rule is intended to deter improper police conduct, it should not be applied in cases where the deterrence purpose is not served....” *Casillas*, ¶21. It would not be served here. *Nix*, 467 U.S. at 444 (The inevitable discovery exception is appropriate

where “the deterrence rationale has so little basis that the evidence should be received.”).

Alternatively, if this case is remanded, the trial court should have the opportunity to make findings as to whether the warrant was properly executed due to D.C.’s and B.C.’s “ability to access” Dhyne’s room, *see Webb*, ¶9, which the prosecution had no need to pursue after the trial court had denied the suppression motion, which occurred *before* Dhyne began to assert his theory that they had access to his room. Or, in its discretion, the trial court should consider any other appropriate exclusionary rule exceptions, such as the good faith exception. *Tallent*, ¶10 (holding the trial court did not abuse its discretion by entertaining new arguments on remand following the defendant’s successful challenge to an order denying suppression and his subsequent conviction); *but see People v. McKnight*, 2019 CO 36, ¶61 (considering exclusionary rule arguments not made in the suppression hearing waived).

CONCLUSION

This Court should affirm because the detective's execution of the warrant was objectively reasonable. Alternatively, the trial court properly applied the inevitable discovery exception to the exclusionary rule.

PHILIP J. WEISER
Attorney General

s/ Trina K. Kissel _____
TRINA K. KISSEL, 47194*
Senior Assistant Attorney General
Criminal Appeals Section
Attorneys for Appellee
*Counsel of Record

CERTIFICATE OF SERVICE

This is to certify that I have duly served the within PEOPLE'S ANSWER BRIEF upon ADAM TUCKER and all parties herein, via Colorado Courts E-filing System on February 1, 2024.

s/ Trina K. Kissel _____