SUMMARY
October 20, 2022

2022COA122

No. 20CA1565, *People v. Dhyne* — Constitutional Law — Fourth Amendment — Searches and Seizures — Warrantless Search — Multiple Occupancy Structures — Common Use or Occupation Exception

A division of the court of appeals considers the circumstances under which a warrant that lists a physical address and identifies an IP address associated with that physical address may be valid to search a separate residence located at the same address. Applying the rule of common use or occupation, the majority concludes that the search of a separate residence fell within the scope of the warrant based on information that the IP address that formed the basis for probable cause was shared. Therefore, it affirms. The special concurrence would affirm the trial court's suppression order based on the entire premises being suspect.

COLORADO COURT OF APPEALS **2022COA122**

Court of Appeals No. 20CA1565
Clear Creek County District Court No. 17CR76
Honorable Catherine J. Cheroutes, Judge

The People of the State of Colorado,

Plaintiff-Appellee,

v.

Kevin Matthew Dhyne,

Defendant-Appellant.

JUDGMENT AFFIRMED

Division IV
Opinion by JUDGE PAWAR
Brown, J., concurs
Richman, J., specially concurs

Announced October 20, 2022

Philip J. Weiser, Attorney General, Trina K. Kissel, Assistant Attorney General, Denver, Colorado, for Plaintiff-Appellee

Law Office of Adam Tucker, P.C., Adam M. Tucker, Michael S. Sager, Jason C. Fisher, Denver, Colorado, for Defendant-Appellant

¶ 1 Defendant, Kevin Matthew Dhyne, appeals his judgment of conviction for two counts of sexual exploitation of a child. We affirm.

I. Background

¶ 2 A detective discovered that child pornography was being downloaded to an Internet Protocol (IP) address assigned to an internet subscriber in his jurisdiction. Upon further investigation, the officer learned that the subscriber's son, B.C., lived with the subscriber and was a registered sex offender.

¶ 3 Based on this information, the officer obtained a search warrant describing "computer and computer systems . . . [b]elieved to be situated on the person, place, or vehicle known as: House, garage, and any outbuildings located at [the subscriber's address]." The affidavit provided in support of the warrant stated the officer's belief that there was probable cause that computers located at this physical address may contain images of child pornography and that B.C. was a possible suspect.

¶ 4 The warrant was issued, and police went to the subscriber's house to execute it. While outside the property, they encountered Dhyne, who had emerged from what appeared to be a basement

dwelling unit in the house. Dhyne told the officers that he rented the basement apartment and shared internet access with the subscriber.

¶ 5 Police searched the premises, including Dhyne's apartment. They seized several computers, including a laptop Dhyne admitted was his property. A later search of this computer revealed sexually exploitative material involving children.

¶ 6 Dhyne was charged with two counts of sexual exploitation of a child. Before trial, he moved to suppress the material found on his computer, arguing it was discovered in violation of his Fourth Amendment right to be free from unreasonable searches. The district court denied the motion. Although the court concluded that the search of Dhyne's apartment exceeded the scope of the warrant, it nevertheless concluded that the material found on his computer was admissible because it would have inevitably been discovered through lawful means.

¶ 7 Dhyne also filed a notice regarding his intent to introduce alternate suspect evidence related to B.C. The court ruled the evidence was not admissible because there was no suggestion that

B.C. had accessed Dhyne's computer and because B.C.'s status as a sex offender was more prejudicial than probative under CRE 403.

¶ 8 The district court conducted a bench trial and found Dhyne guilty as charged. Dhyne now appeals.

II. Motion to Suppress

¶ 9 Dhyne argues the district court misapplied the inevitable discovery exception to the Fourth Amendment's exclusionary rule and erred by denying his motion to suppress. The State asserts the search of Dhyne's apartment was lawful and that, in any event, the inevitable discovery exception applies. We need not address the inevitable discovery issue because we conclude that, under the circumstances of this case, the search did not exceed the scope of the warrant.

A. Applicable Law

¶ 10 The Fourth Amendment provides that individuals shall be free from unreasonable searches and seizures. U.S. Const. amend. IV. A warrantless search of a person's home is presumptively unreasonable and therefore illegal. *People v. Dyer*, 2019 COA 161, ¶ 15. To be valid, a warrant must be issued "upon probable cause supported by oath or affirmation particularly describing the place to

be searched and the things to be seized." *People v. Martinez*, 165 P.3d 907, 909 (Colo. App. 2007); *see also Maryland v. Garrison*, 480 U.S. 79, 85 (1987) ("[W]e must judge the constitutionality of [police officers'] conduct in light of the information available to them at the time they acted.").

¶ 11 Where police seek to search a particular unit in a multi-unit building, the Fourth Amendment's particularity requirement generally requires a warrant to "sufficiently describe the apartment or subunit 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) (holding that a warrant that "merely describes the entire multiple-occupancy structure by street address only, without reference to the particular dwelling unit or units sought to be searched," is insufficient).

¶ 12 An exception to this rule applies where the officers conducting the search did not know that the area to be searched contained separate units until after the search began. *People v. Lucero*, 174 Colo. 278, 280-81, 483 P.2d 968, 970 (1971). Whether the *Lucero* exception applies "turns on an objective examination of whether the facts known to the police suggested that the premises to be

searched contained more than one dwelling unit." *Martinez*, 165 P.3d at 911.

> [W]here a significant portion of the premises is used in common and other portions, while ordinarily used by but one person or family, are an integral part of the described premises and are not secured against access by the other occupants, then the showing of probable cause extends to the entire premises.

Id. (quoting 2 Wayne R. LaFave, *Search and Seizure* § 4.5(b), at 529 (3d ed. 1996)). "In the community-occupation situation, . . . courts have held that a single warrant describing the entire premises so occupied is valid and will justify search of the entire premises." 2 Wayne R. LaFave, *Search and Seizure* § 4.5(b), at 725 (6th ed. 2020) (collecting cases).

¶ 13 A trial court's ruling on a motion to suppress presents a mixed question of fact and law. *Martinez*, 165 P.3d at 909. We must defer to the trial court's findings of fact if they are supported by competent evidence in the record, but we review its conclusions of law de novo. *Id.* We may affirm a trial court's suppression ruling on any grounds supported by the record. *People v. Stock*, 2017 CO 80, ¶ 13.

B. Discussion

¶ 14 This appeal presents a unique question: Where a warrant authorizes the search of a physical address based on its association with a specific IP address, and police discover before executing the warrant that the physical address contains a primary residence and a separate residence, each of which can access the IP address that formed the basis for probable cause, is a search of the separate residence authorized? Under the circumstances before us, we conclude it is.

¶ 15 The particular place authorized to be searched in this case was any area within the subscriber's physical address from which the IP address could be accessed. At the time police obtained a warrant, they "had every reason to believe that the house was a one-family residence." *Lucero*, 174 Colo. at 281, 483 P.2d at 970 (identifying an exception to *Avery*'s requirement for separate warrants for separate units). But police obtained new information between obtaining the warrant and executing the search.

¶ 16 When Dhyne encountered police outside the house, he told them that he (1) rented a separate unit in the basement and (2) used the same IP address as the subscriber. In our view, this

second piece of information is critical. It gave the police reason to believe that the area to be searched — the parts of the physical address from which the IP address could be accessed — was "used in common" and "not secured against access by the other occupants." *Martinez*, 165 P.3d at 911 (quoting 2 LaFave, § 4.5(b), at 529 (3d ed. 1996)). Because 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.

¶ 17 Our holding is narrow, based on the facts before us and application of the law articulated in *Martinez*.[1] *See id.* at 912 (holding that "ready access" to a shared space identified in the search warrant justified search irrespective of whether the officers

---

[1] While we recognize *Martinez* was based on the common occupation of physical premises, we conclude its rationale also applies to the common or shared use of an IP address. *See People v. Martinez*, 165 P.3d 907, 911 (Colo. App. 2007) (citing law related to "the described premises" in the warrant); *see also State v. Mansor*, 421 P.3d 323, 340-41 (Or. 2018) (applying the particularity requirement to search of a computer, notwithstanding the fact that the requirement "developed in a world of physical evidence rather than in the digital context").

were aware that the defendant maintained a separate residence); *see also People v. Alarid*, 174 Colo. 289, 293, 483 P.2d 1331, 1332-33 (1971) (holding, in a case announced on the same day as *Lucero*, that, by contrast, where officers had reason to know that the house to be searched contained more than one unit and "no facts were presented which would show that there was probable cause to believe that criminal activity was occurring in both dwelling places," a general search of the house "went beyond the area which [police] had probable cause to search").

¶ 18 The special concurrence would affirm under different reasoning, relying on *United States v. Axelrod*, No. WDQ-10-0279, 2011 WL 1740542 (D. Md. May 3, 2011), a nonbinding and unpublished order from the United States District Court for the District of Maryland. Initially, we note that the district court in *Axelrod* determined that the search was authorized because the officers did not know that Axelrod maintained a separate residence — facts that are distinguishable from ours. The *Axelrod* court went on to determine in the alternative, however, that even if the officers had known that Axelrod maintained a separate residence, the search was valid. It did so based on a finding that the IP address

was shared because "the internet connection was open and anyone in the residence could access it."[2] *Id.* at *5.

¶ 19 The special concurrence relies on *Axelrod*'s alternative ruling to conclude that the search of Dhyne's separate residence was authorized, not because of the common occupation rule, but because, given the nature of the evidence police were searching for, "the entire premises [were] suspect." *Infra* ¶ 41 (quoting *United States v. Whitney*, 633 F.2d 902, 907 n.3 (9th Cir. 1980), in turn citing Annotation, 22 A.L.R.3d 1330, 1340-47 (1967 & Supp. 1980)).[3] We find it unnecessary to rely on this secondary authority because our own case law allows us to reach the correct result.

---

[2] The *Axelrod* court appears to have based this finding on a police officer's testimony that he observed a wireless router on the steps outside of Axelrod's room that "took 'the hard connection of the Internet from the cable and boost[ed] the signal'" so that other devices could use that signal to connect to the internet. *United States v. Axelrod*, No. WDQ-10-0279, 2011 WL 1740542, *2 (D. Md. May 3, 2011) (unpublished opinion). Whether we would reach the same legal conclusion on these facts is not before us; rather, we simply note that the court's ruling in *Axelrod* is similarly based on a finding of common use of the IP address.

[3] It appears *United States v. Whitney*, 633 F.2d 902, 907 n.3 (9th Cir. 1980), contains a volume-number typo and intended to cite W. C. Crais III, Annotation, *Search Warrant: Sufficiency of Description of Apartment or Room to be Searched in Multiple-Occupancy Structure*, 11 A.L.R.3d 1330, 1340-47 (1967 & Supp. 1980).

And we see no other reason to depart from *Avery*'s general rule, *Lucero*'s exception, and *Martinez*'s holding regarding common occupancy situations — all of which require some information upon which a trial court can find that the expanded search falls within the scope of the warrant.[4] *See People v. Eirish*, 165 P.3d 848, 852 (Colo. App. 2007) ("Probable cause must be established with respect to *each place* to be searched.") (emphasis added); *see also Whitney*, 633 F.2d at 907 ("The command to search can never include more than is covered by the showing of probable cause to search." (quoting *United States v. Hinton*, 219 F.2d 324, 325 (7th Cir. 1955))).

¶ 20 Because Dhyne informed police that he shared the IP address associated with the physical address identified in the warrant, his residence fell within its scope. Accordingly, we affirm the suppression order, though on different grounds than those relied upon by the district court. *Stock*, ¶ 13.

---

[4] The special concurrence acknowledges that the reason the entire premises were suspect was because Dhyne admitted to using the subscriber's IP address. *See infra* ¶ 50. Without that admission (or some other information showing that the IP address was shared), Dhyne's separate residence would not have fallen within the warrant's showing of probable cause. *Martinez*, 165 P.3d at 912.

III. Alternate Suspect Evidence

¶ 21 Dhyne also asserts that the district court violated his right to present a defense by denying his request to introduce evidence that B.C. was an alternate suspect. We disagree.

A. Applicable Law

¶ 22 A criminal defendant is entitled to all reasonable opportunities to present evidence that might tend to create doubt as to the defendant's guilt, including evidence of an alternate suspect. *People v. Elmarr*, 2015 CO 53, ¶¶ 26, 29. "However, the right to present a defense is generally subject to, and constrained by, familiar and well-established limits on the admissibility of evidence." *Id.* at ¶ 27.

¶ 23 "To be admissible, alternate suspect evidence must be relevant (under CRE 401) and its probative value must not be sufficiently outweighed by the danger of confusion of the issues or misleading the jury, or by considerations of undue delay (under CRE 403)." *Id.* at ¶ 22. "The touchstone of relevance in this context is whether the alternate suspect evidence establishes a non-speculative connection or nexus between the alternate suspect and the crime charged." *Id.* at ¶ 23. "Whether the requisite connection exists requires a case-

by-case analysis, taking into account all of the evidence proffered by the defendant to show that the alternate suspect committed the charged crime." *Id.* at ¶ 32.

¶ 24 In balancing the probative value of alternate suspect evidence against the countervailing policy considerations of CRE 403, a reviewing court must afford the evidence the maximum probative value attributable by a reasonable fact finder and the minimum unfair prejudice to be reasonably expected. *Id.* at ¶ 44 ("The probative worth of any particular bit of evidence is affected by the scarcity or abundance of other evidence on the same point.").

¶ 25 Trial courts have broad discretion in determining the admissibility of evidence, including alternate suspect evidence, based on its relevance, probative value, and prejudicial impact. *Id.* at ¶ 20. We will reverse the court's evidentiary ruling only where it is manifestly arbitrary, unreasonable, or unfair, or based on an erroneous view of the law. *Id.*

B. Discussion

¶ 26 Dhyne argues the district court erred by denying his request to introduce alternate suspect evidence because there was a sufficient nexus between B.C. and the charged crimes to make this

evidence relevant. Specifically, he points to evidence that B.C. lived at the same address as Dhyne, had a conviction for a sexual offense involving a minor, and had been identified as a person of interest for the charged crimes by law enforcement and named in the affidavit supporting the search warrant. He further argues that, because a search of B.C.'s computer was inconclusive, B.C. cannot be excluded as an alternate suspect. We perceive no error in the district court's exercise of its discretion.

¶ 27 The evidence Dhyne relies upon suggests that B.C. had a motive (as a sex offender who enjoyed watching pornography) and opportunity (as Dhyne's neighbor) to commit the charged offenses. But as our supreme court has observed,

> evidence merely showing that someone else had a motive or opportunity to commit the charged crime — without other additional evidence circumstantially or inferentially linking the alternate suspect to the charged crime — presents too tenuous and speculative a connection to be relevant because it gives rise to no more than grounds for possible suspicion.

Elmarr, ¶ 34.

¶ 28 Dhyne points to no evidence linking B.C. to the charged offenses beyond his motive and opportunity. Dhyne argues that it

is reasonable to assume that the internet subscriber would have had a key to Dhyne's space, as his landlord, and that B.C., as the subscriber's son, would have "at least know[n] where that key was located" and therefore could have accessed Dhyne's computer and downloaded child pornography. But these assumptions are speculative and insufficient to make an alternate suspect connection.[5] *Id.* at ¶ 32. Accordingly, on the facts presented to the district court, we conclude the alternate suspect evidence was properly excluded.

IV. Sufficiency of the Evidence

¶ 29 Finally, Dhyne challenges the sufficiency of the evidence to support his convictions. We conclude the evidence was sufficient.

A. Applicable Law

¶ 30 We review the record de novo to determine whether the evidence was substantial and sufficient to support a conclusion by

---

[5] Dhyne's suggestion that the search of B.C.'s computer was inconclusive and thus may have turned up child pornography was not presented to the district court. In any event, we conclude this evidence, too, is speculative, and the failure to consider it was not error, let alone plain error. *See People v. Ujaama*, 2012 COA 36, ¶ 42 ("To qualify as plain error, the error must be one that 'is so clear-cut, so obvious,' a trial judge should be able to avoid it without benefit of objection.") (citation omitted).

a reasonable mind that the defendant is guilty of the charge beyond a reasonable doubt. *See People v. Donald*, 2020 CO 24, ¶ 18; *People v. Garcia*, 2022 COA 83, ¶ 16. In doing so, we view the evidence as a whole and in the light most favorable to the prosecution, giving the prosecution the benefit of all reasonable inferences that might fairly be drawn from the evidence. *Id.* at ¶¶ 18-19. "[I]f there is evidence upon which one may reasonably infer an element of the crime, the evidence is sufficient to sustain that element . . . ." *People v. Kessler*, 2018 COA 60, ¶ 12 (quoting *People v. Chase*, 2013 COA 27, ¶ 50).

¶ 31 A person commits sexual exploitation of a child if he knowingly possesses or controls any sexually exploitative material for any purpose. § 18-6-403(3)(b.5), C.R.S. 2022. "A person acts 'knowingly' . . . with respect to conduct or to a circumstance described by a statute defining an offense when he is aware that his conduct is of such nature or that such circumstance exists." § 18-1-501(6), C.R.S. 2022.

¶ 32 The state of mind element of an offense "is normally not subject to direct proof and must be inferred from [the defendant's] actions and the circumstances surrounding the occurrence."

Kessler, ¶ 12; *see Donald*, ¶ 37 (noting that knowledge may be inferred from circumstantial evidence).

B. Discussion

¶ 33 At trial, the investigating officer testified that after encountering Dhyne outside the house, Dhyne asked to go back into his apartment to get some cigarettes and, while inside, pointed out several computers as belonging to him. One of these laptops contained at least one video and more than twenty images that the parties stipulated were sexually exploitative. It also contained at least 241 files that appeared to be child pornography. An expert witness testified that the presence of the sexually exploitative video on the computer "was definitely not an anomaly" and "was very consistent to a large amount of data and artifacts that were found from other locations of the computer that . . . show a pattern — a definite pattern of interest in files of that type."

¶ 34 Viewing this evidence in the light most favorable to the prosecution, we conclude the fact finder could reasonably infer from Dhyne's actions and the circumstances surrounding the occurrence that he knowingly possessed sexually exploitative material. *Kessler*, ¶ 12. While Dhyne argues the prosecution failed to show that he

downloaded the video and images with the intent to use them for an unlawful purpose, the statute criminalizes possession of these types of files for "any purpose." § 18-6-403(3)(b.5). Accordingly, we conclude the evidence was sufficient to support Dhyne's convictions.

V. Conclusion

¶ 35 The judgment is affirmed.

JUDGE BROWN concurs.

JUDGE RICHMAN specially concurs.

JUDGE RICHMAN, specially concurring.

¶ 36 I agree with both the result the majority reaches and most of their rationale. Nonetheless, I write separately because, in my view, the so-called "common occupation" exception is not the appropriate legal lens through which to analyze the search in this case.

¶ 37 The common occupation exception has historically been applied, as in *People v. Martinez*, 165 P.3d 907 (Colo. App. 2007), to the shared use of a physical location, like a room in a house. The majority, however, stretches the doctrine to account for the shared use of what I can only describe as a "metaphysical" location, the IP address assigned to the subscriber. According to the majority, the officers' search of Dhyne's basement unit was permissible not because anyone else — for example, B.C. — had access to the unit, but because Dhyne used or "occupied in common" the IP address used at the house described in the warrant. But how does one "occupy" an IP address?

¶ 38 I respectfully submit that this case can be resolved without engaging in such semantic contortions.

¶ 39 As the Ninth Circuit explained in *United States v. Whitney*, 633 F.2d 902, 907 (9th Cir. 1980), when a building is divided into more

than one unit, probable cause must exist for each unit to be searched, and the general rule in such instances is that a warrant that describes an entire building when cause is shown for searching only one unit is void.

¶ 40 But, as the court further explained, there are multiple exceptions to the general rule, including "situations where [(1)] the premises are occupied in common rather than individually, [(2)] the defendant was in control of the whole premises, [(3)] *the entire premises are suspect*, or [(4)] the multiunit character of the premises is not known or apparent to the officers . . . executing the warrant." *Id.* at 907 n.3 (emphasis added); *see also United States v. Gilman*, 684 F.2d 616, 618 (9th Cir. 1982) (recognizing the same exceptions).

¶ 41 Thus, the "common occupation" exception is but one of several exceptions to the general rule about searching a multi-unit building. Therefore, I would not force the facts of this case, involving, as they do, a search for pornography maintained on a computer, into the common occupation exception when another exception will do. And I think another exception — namely, the "entire premises are suspect" exception — will do. Although

Colorado courts have neither adopted this exception nor applied it to the scope of a search related to an IP address, a handful of federal cases persuade me that this is the correct approach.

¶ 42 I begin with a case from the United States District Court for the District of Maryland that upheld a search in a factual scenario nearly identical to the one in this case.

¶ 43 In *United States v. Axelrod*, No. WDQ-10-0279, 2011 WL 1740542, at *1 (D. Md. May 3, 2011) (unpublished opinion), the police learned that an IP address assigned to an internet subscriber at a specific street address was sharing files that appeared to contain child pornography. Police then obtained a warrant to search the house at the street address for evidence of distribution, production, or possession of child pornography.

¶ 44 When the police executed the warrant, they met the subscriber's wife at the front door and explained to her the purpose of the warrant. *Id.* One of the officers then walked into a laundry room and through a second door that led to a staircase at the back of the house. *Id.* The staircase, in turn, led to a room above the garage, described in the order as "part of an in-law suite" rented by the defendant and his cousin. *Id.* At the top of the stairs was a

wireless router, and the defendant was in the suite. *Id.* The police entered the suite, seized the defendant's computers, searched the computers, and found child pornography. *Id.* at *2. The defendant was charged with distribution and receipt of child pornography as well as possession of child pornography. *Id.*

¶ 45 Before trial, the defendant moved to suppress the evidence obtained from his computers. *Id.* At the suppression hearing, the officer who first entered the suite testified that when he entered the suite, he did not know it was a separate residence. *Id.* For her part, the subscriber's wife testified that, as far as she recalled, she had told the officers prior to their entering the suite that it was separate from the main house and was being rented by the defendant and his cousin. *Id.*

¶ 46 In denying the defendant's motion to suppress, the district court made several statements equally applicable to the search at issue in this case. First, it stated, consistent with Colorado law, that "the Fourth Amendment is violated if officers searching a multi-unit property do not discontinue their search upon discovering that they are in a unit 'erroneously included within the terms of the warrant' — i.e.[,] a unit for which the issuing

magistrate has not made a probable cause determination." *Id.* at *4 (quoting *Maryland v. Garrison*, 480 U.S. 79, 87 (1987)).

¶ 47 The court then recited the four exceptions to the general rule about searching a multi-unit building. *Id.* Even assuming the subscriber's wife had told the officers that the defendant rented the in-law suite before they searched it, the court reasoned, suppression was not required because the warrant could reasonably be interpreted as providing probable cause to search the suite. *Id.* at *5. Why? Because "the entire premises were suspect" given that "the internet connection was open and anyone in the residence could access it." *Id.*

¶ 48 The court noted that the language of the warrant "did not limit the search to the [subscriber and subscriber's wife's] portion of the residence, or indicate that [they] were the targets of the investigation." *Id.* Moreover, the court observed that, as in this case, the affidavit supporting the warrant merely indicated that an unknown "computer user at the location associated with the suspect IP address had downloaded and distributed child pornography." *Id.* Thus, the court reasoned, the officers who searched the subscriber's house reasonably believed that the

warrant authorized them to search the entire premises, including the in-law suite. *Id.*

¶ 49 In addition to *Axelrod*, I am persuaded by the reasoning of a case cited therein, *United States v. Tillotson*, No. 2:08-CR-33, 2008 WL 5140773, at *2 (E.D. Tenn. Dec. 2, 2008) (unpublished opinion). In short, *Tillotson* is another child pornography case in which the defendant sought to suppress evidence that police found on his computer during a search of his residence. *Id.* As in *Axelrod*, the defendant lived in a house with multiple occupants, and all that federal agents knew before searching the house was that an IP address assigned to an internet subscriber at the house's street address was sharing files that appeared to contain child pornography. *Id.* at *2-3. In rejecting the defendant's argument that, considering the number of people who lived in the house, the search warrant was not sufficiently "tailored," the court stated:

> What defendant's argument overlooks is that the United States had probable cause to believe that a computer located in the residence at [street address] was being used to transmit and receive images of child pornography. As far as the United States knew, *any* of the occupants of [street address] — or all of them, for that matter — could have used the computer to send and receive child

> pornography. Having no knowledge where the computer (or computers) and other electronic storage devices might be located, [the federal agent] reasonably was authorized to search throughout the entire house. . . . The search warrant was as "tailored" as it could be under the circumstances.

Id. at *7; *see also United States v. Massey*, No. 4:09CR506-DJS, 2009 WL 3762322, at *6 n.2 (E.D. Mo. Nov. 10, 2009) ("Police officers discovered that a user of a specific IP address possessed child pornography. That IP address was then linked to a specific physical residence. Therefore, there existed a fair probability that child pornography would be found at that residence to support the Search Warrant.").

¶ 50 Turning back to this case, I agree with my colleagues that Dhyne's Fourth Amendment rights were not violated when the officers searched the unit where he was living. I simply write to suggest a different reason for that conclusion. Given the nature of the evidence that the officers were searching for and the information they had about the subscriber's house, the entire premises were suspect, including Dhyne's unit, once he admitted to using the subscriber's IP address.