Colorado Supreme Court **Two East 14th Avenue** **Denver, Colorado 80203**	
On Writ of Certiorari to: Colorado Court of Appeals Opinion by Pawar, J.; Brown, J., concurring; Richman, J., specially concurring. Case No. 2022 COA 122	
Kevin Matthew Dhyne Defendant-Appellant *v.* **The People of the State of Colorado** Plaintiff-Respondent	**△ Court Use Only △**
Attorneys for Amici Curiae Professors of Law & Engineering Vivek Krishnamurthy (Law. Prof. Reg. #58996) Sebastian Blitt (Student Attorney) Madeline Finlayson (Student Attorney) Sarah Misché (Student Attorney) University of Colorado Law School Clinical Programs Wolf Law Building | 404 UCB 2450 Kittredge Loop Drive Boulder, CO 80309 (303) 492-0209 vivek.krishnamurthy@colorado.edu	**Case No.** 22SC869
Brief of *Amici Curiae* Professors of Law & Engineering in Support of Neither Party	

Certificate of Compliance

I hereby certify that this brief complies with the requirements of C.A.R. 28, 29, and 32, including all applicable formatting requirements set forth in these rules. The brief complies with C.A.R. 28 as it contains 3373 words.

/s/ Vivek Krishnamurthy
Attorneys for *Amici Curiae* Professors of Law & Engineering

Vivek Krishnamurthy (Law Prof. Reg. #58996)
Sebastian Blitt (Student Attorney)
Madeline Finlayson (Student Attorney)
Sarah Misché (Student Attorney)

University of Colorado Law School Clinical Programs
Wolf Law Building | 404 UCB
2450 Kittredge Loop Drive
Boulder, Colorado 80309
(303) 492-0209
vivek.krishnamurthy@colorado.edu

Table of Contents

Table of Authorities

Colorado Cases

Federal Cases

State Cases

Colorado Constitutional Provisions

Federal Constitutional Provisions

Other Authorites

Identity and Interest of Amici Curiae

Amici are professors of law and engineering who teach and write about internet technology and related subjects. They submit this amicus curiae brief in support of neither party to inform the Court and the parties of developments in internet technology that are germane to the legal issues raised in this appeal.

Vivek Krishnamurthy is an Associate Professor of Law and Director of the Samuelson-Glushko Technology Law & Policy Clinic at the University of Colorado Boulder.

Blake Reid is an Associate Professor of Law at the University of Colorado Boulder.

Eric Wustrow is an Associate Professor of Electrical, Computer, and Energy Engineering at the University of Colorado Boulder.

Summary of the Argument

Courts have long assumed that an association between an IP address and criminal activity furnished an appropriate basis for authorizing the search of the premises associated with the IP address for evidence of crime. However, technological changes have weakened these associations over time. Today, home internet connections are shared between dozens of "smart" devices, while the rise of wireless networking technology allows one's friends and neighbors—or even complete strangers—to access one's internet connection. Furthermore, computing devices have become increasingly mobile, and can connect to the internet from different locations throughout the day. Taken together, these changes mean that more devices, used by different people, across different locations, can all share one internet connection—and therefore be associated with the same IP address.

This case presents this Court with an opportunity to consider how and when searches of physical locations for electronic devices containing evidence of crime should be authorized when there is an association between an IP address and criminal activity. While *amici* take no view on the outcome of this appeal, they believe that the public interest is best served by adopting a "totality of the circumstances" analysis. Such an analysis is best suited to ensuring that search warrants in cases involving an association between an IP address and

criminal activity meet the constitutional requirements of probable cause and particularity.

Argument

1. The ability of IP addresses to identify physical locations to search for electronic evidence of crime has diminished over time.

Internet Protocol (IP) addresses are numerical addresses assigned to devices connected directly to the internet.[1] They allow such devices to communicate with each other by ensuring that information is sent to the correct destination among the billions of devices that are connected to the internet at any given time. James Grimmelmann, *Internet Law: Cases & Problems* 30 (Lydia P. Loren & Joseph S. Miller eds., 13th ed. 2023).

IP addresses must be unique to serve this function. Michael Dooley & Timothy Rooney, *IP Address Management* 51 (Thomas Plevyak, et al. eds., 2d ed. 2021). To accomplish this, a non-profit called the Internet Assigned Numbers Authority (IANA) coordinates the distribution of IP addresses to five "regional internet registries" that serve the major regions of the world. *Id.* at 51-52. Specifically, IANA calculates the number of IP addresses that each region needs and allocates them to the relevant regional registry. *Id.* at 52. In the United States, ARIN—

[1] We used the expression "connected directly" to refer to devices that are assigned publicly routable IP addresses by an internet service provider. This contrasts with devices that are connected "indirectly" to the internet through a home router to permit the sharing of an internet connection, which results in many devices exhibiting the same public IP address. *See* discussion *infra* at pp. 12-14.

the regional registry for North America—allocates the IP addresses it receives from IANA to various internet service providers (ISPs) across the country, such as Xfinity (Comcast) or Verizon. *Id.* at 52-53.

American ISPs then assign a unique IP address from the allocation they receive from ARIN to each of their subscribers. *Id.* In the typical residential setup, an ISP assigns the subscriber with an IP address when the subscriber's modem connects to the ISP's network. *Id.* at 58-61. Such IP addresses are known as "public," meaning these addresses can be used by other internet-connected devices to transmit digital information to the correct online resource. *Id.* at 38-39.

Criminal investigations into illicit online activity often begin with law enforcement receiving a tip about such activity. This is illustrated in *People v. N.T.B.*, 2019 COA 150, where an online storage provider (Dropbox) suspected that one of its accounts contained an illicit video. Dropbox sent a copy of the video in question, along with the IP address associated with the upload—which its systems had automatically logged—to the National Center for Missing and Exploited Children (NCMEC). *Id.* at ¶ 2. In turn, NCMEC forwarded this information to local police, who traced the IP address to a specific ISP using public databases. *Id.* at ¶¶ 2-3. Typically, ISPs maintain logs of the IP addresses assigned to individual subscribers for six to nine months. Colleen M. Devanney & Jordan S. Cohen, *Utilizing IP Addresses to Subpoena Internet Service Providers (ISPs)*, Lexology (May

31, 2016), https://www.lexology.com/library/detail.aspx?g=1d6d39a3-db07-4d1d-a017-0c7e6cd5c973 [https://perma.cc/A9WE-7GPS]. Therefore, the police were able to subpoena the ISP for the name and address of the subscriber who was assigned the IP address at the time of the suspected criminal activity. *N.T.B.*, ¶ 3. The information obtained through the subpoena enabled the police to seek a search warrant to search the internet subscriber's home for the illicit materials in question. *Id.* at ¶¶ 3-4.

In recent years, internet technology has evolved in ways that weaken the association between an IP address associated with criminal activity and a physical address obtained from an ISP. As explained below, more devices share the same internet connection, more users connect to the internet wirelessly, and devices which connect to the internet have become increasingly mobile. These dynamics all serve to attenuate the connection between an IP address and the likelihood of finding electronic evidence of crime at the subscriber's physical address.

1.1. The association between IP addresses and physical addresses has become more imperfect over time as an increasing number of devices share the same internet connection.

In the early days of the internet, it was extremely difficult for more than one device to use a residential internet connection at a time. For

example, in 2003, sixty-nine percent of Americans with internet access used dial-up technology to get online, which allows a computer equipped with a modem to connect to the internet through a phone line. John B. Horrigan, *Broadband Adoption at Home*, Pew Rsch. Ctr. (May 18, 2003), https://www.pewresearch.org/internet/2003/05/18/broadband-adoption-at-home. Due to the limited bandwidth available on dial-up connections and other technical considerations, there was almost always a one-for-one association between a public IP address assigned by an ISP, and a particular computer accessing the internet from a particular phone line. This technological landscape informed the outcome of cases such as *United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003), which stated that IP addresses are "the unique address assigned to a particular computer connected to the internet." *Id.* at 1042 (quoting Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1145 (2002)).

Internet technology has changed considerably in the intervening years, however. Consider the typical American home, which in 2023 contained an average of 21 internet-connected devices, such as laptop computers, tablets, smartphones, "smart" TVs, and video game consoles. Jana Arbanas et al., *Connected Consumer Survey 2023,* Deloitte, https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey.html

[https://perma.cc/UT9V-NWH3] (last visited Nov. 1, 2023). These devices don't typically have their own direct, dedicated connection to the internet, as in the dial-up era of the late 1990s and early 2000s. Rather, modern home internet routers allow dozens or even hundreds of digital devices to share the same home internet connection, thanks to the development of a technology known as "network address translation." Dan Wing, *Network Address Translation: Extending the Internet Address Space*, IEEE Internet Computing, July-Aug. 2010, at 66, 66-67 (available at https://doi.org/10.1109/MIC.2010.96). Today, most personal electronic devices connect to the internet *indirectly* through a home router that permits numerous devices to share a public IP address, rather than *directly* with a unique public IP address as in the days of dial-up internet access. The use of home routers to share internet connections results in the public IP address assigned by an ISP to a subscriber now being shared by many different devices. All such devices will exhibit the same public IP address to the outside world. *Id.*

Since many devices now share the same public IP address, it is no longer appropriate to assume that IP addresses are "the unique address assigned to a particular computer connected to the internet." *Steiger*, 318 F.3d at 1042 (quoting Solove, *supra*) (cited with approval in *People v. Garrison,* 2017 COA 107 at ¶ 24 n.3, and *People v. N.T.B,* ¶ 2 n.2). In the current technological context, a subpoena directed at an ISP 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*. Correspondingly, courts can no longer assume that "once law enforcement has an IP address, it can easily associate that IP address with an *individual*." *People v. Seymour*, 2023 CO 53, ¶ 31 (emphasis added).

As explained in further detail below, however, an IP address is less likely today than it was a decade ago to identify either the individual(s) who committed the crime or the device(s) they used to do so. These distinctions are important, because two other technological developments—the rise of wireless networking and the increasing portability of digital devices—also have implications for the association between IP addresses, physical locations, and electronic devices containing evidence of crime.

1.2. The growing prevalence of wireless networking technology has attenuated the association between IP addresses and physical addresses.

During the era of dial-up internet, there was a strong association between an IP address and a physical address because a computer's modem had to be physically wired into a phone jack to connect to the internet. Today, however, more than 92% of American households with internet access use routers incorporating wireless networking ("Wi-

Fi") capabilities to share a single home internet connection among their numerous devices. *Parks Associates: 92% of US Internet Households Use Wi-Fi at Home, and More than One-Fourth Value Service Quality Over Price*, PR Newswire (Jan. 23, 2023, 8:14 AM), https://www.prnewswire.com/news-releases/parks-associates-92-of-us-internet-households-use-wi-fi-at-home-and-more-than-one-fourth-value-service-quality-over-price-301728088.html [https://perma.cc/4KSD-V8LY].

Under ideal circumstances, Wi-Fi signals can travel up to 550 meters (1800 feet) from a router. Zayan El Khaled et al., *WiFi Coverage Range Characterization for Smart Space Applications*, *in* 2019 IEEE/ACM 1st Int'l Workshop on Software Eng'g Rsch. & Pracs. for the Internet of Things (SERP4IoT) 61, 65 (2019), https://doi.org/10.1109/SERP4IoT.2019.00018. This permits a typical home internet connection to be accessed from beyond the metes and bounds of the typical urban or suburban property, which is why people living in such areas will see many of their neighbors' Wi-Fi networks appear on their digital devices when they attempt to initiate a Wi-Fi connection.

Furthermore, while many Wi-Fi networks are password-protected, "open" or "public" Wi-Fi networks can be used by anyone within range of the Wi-Fi router to connect to the internet—regardless of whether they live at the subscriber's address. Erin Larson, *Tracking Criminals with Internet Protocol Addresses: Is Law Enforcement Correctly*

Identifying Perpetrators?, 18 N.C.J.L. & Tech. 316, 336 (2017); *Open Wireless,* Electronic Frontier Foundation, https://www.eff.org/issues/open-wireless (last visited Nov. 2, 2023).

These technological developments have significant implications for whether the police will find electronic evidence of a crime committed using a particular internet connection on the subscriber's property, as demonstrated by the recent decision of the California Court of Appeals in *People v. Nguyen,* 12 Cal. App. 5th 574 (Ct. App. 2017). In *Nguyen,* the police identified an IP address that was sharing illicit materials online. *Id.* at 577. The ISP in question responded to a police subpoena by providing the address of the subscriber of the account associated with the IP address. *Id.* In turn, the police obtained a search warrant to search the subscriber's home. *Id.*

While executing the warrant, police discovered that Nguyen lived in a separate residence behind the subscriber's home. *Id.* In analyzing whether the police had probable cause to search Nguyen's residence in addition to the subscriber's, the Court noted that "a single apartment-dweller may broadcast a wireless network signal putting dozens of other residents within its range." *Id.* at 585. The court rejected the assertion that the police had probable cause to search any residence within range of the signal. *Id.* at 586.

1.3. The association between IP addresses and physical addresses has become less reliable as devices have become increasingly mobile.

The increasing portability, capability, and storage capacities of digital devices also reduce the likelihood that a search of a location identified using an IP address will yield evidence of crime. In the dial-up era, computers employed dedicated, wired internet connections and were bulky and difficult to transport. Today, Americans use a variety of lightweight, portable devices for their computing needs. In 2022, more than 83% of Americans could access the internet on their smartphones, tablets, or other mobile devices. *How do Americans Connect to the Internet?*, Pew Charitable Trusts (July 7, 2022), https://www.pewtrusts.org/en/research-and-analysis/fact-sheets/2022/07/how-do-americans-connect-to-the-internet [https://perma.cc/X5R3-48C5]. The portability of these devices reduces the likelihood that one that was used to engage in criminal activity using a particular internet connection will be found at the location associated with the connection. For example, a criminal might use a public internet connection to download illicit material, and then proceed with their daily activities. A search of the address associated with the IP address of the internet connection would in such circumstances yield no evidence of criminal activity.

2. Changes in networking technology impact the probable cause and particularity analyses when search warrants are based on an IP address being associated with criminal activity.

Technological advances in the last two decades permit more people located in a wider range of locations to share a single internet connection. These advances, along with the growing portability of electronic devices, have reduced the likelihood that a search of a location associated with an IP address linked to criminal activity will yield electronic devices containing evidence of crime. Such changes impact the probable cause and particularity analyses that courts must undertake in evaluating warrant applications when the association between an IP address and criminal activity forms some or all of the basis for searching a physical location for electronic devices containing evidence of crime. This is especially so because electronic devices, such as laptop computers and smartphones, contain the "privacies of life," *Riley v. California*, 573 U.S. 373, 403 (2014) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)) and are "deserving of [heightened] protection." *People v. Coke*, 2020 CO 28 at ¶ 36.

The Fourth Amendment requires warrants to be based on "probable cause" and to "particularly" describe "the place to be searched, and the persons or things to be seized." U.S. Const. amend IV. Similarly, the Colorado Constitution provides that "no warrant to search any place or seize any person or things shall issue without

describing the place to be searched, or the person or thing to be seized, as near as may be, nor without probable cause, supported by oath or affirmation reduced to writing." Colo. Const. art. 2, § 7. Probable cause exists when "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983); *People v. Miller*, 75 P.3d 1108, 1112 (Colo. 2003).

The particularity requirement serves the same purpose under both the federal and the state constitution. *People v. Seymour*, 2023 CO 53, ¶ 44. It cabins the government's discretion in examining otherwise private materials by prohibiting "general warrants," which would permit "a general, exploratory rummaging in a person's belongings." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)); *Seymour*, ¶ 44.

The impacts of the changing nature of internet technology on the probable cause and particularity analyses in cases such as the one at bar are best demonstrated by means of two examples.

Let us consider an isolated cabin in the woods with an internet connection whose IP address has been associated with criminal activity. Police observation of the cabin has established that only one person lives there. In this scenario, there is a "fair probability" that the resident of the cabin is the person who used the internet connection to commit a crime, and that a search of the individual's digital devices will yield evidence of crime. *People v. Miller*, 75 P.3d at 1112 .

Now let us consider an investigation where the association between an IP address and criminal activity brings the police to a multi-generational family home in a dense, urban neighborhood where the internet subscriber in question operates an open, public Wi-Fi network. In this case, the "probability that contraband or evidence of a crime will be found" at the subscriber's residence is considerably lower than in the first hypothetical. *See, e.g.*, *Gates*, 462 U.S. at 238. The probability that the device that accessed the subscriber's internet connection for illicit purposes belongs to a neighbor or a passerby is far higher than in the first hypothetical. Furthermore, a search of every device belonging to every resident of the subscriber's home leads to concerns of a "general, exploratory rummaging" of the sort that the particularity requirement is meant to prevent. *Andresen*, 427 U.S. at 480 (quoting *Coolidge*, 403 U.S. at 467); *Seymour*, ¶ 44.

3. A "TOTALITY OF THE CIRCUMSTANCES" ANALYSIS IS BEST SUITED TO EVALUATING THE CONSTITUTIONALITY OF SEARCH WARRANTS IN CASES INVOLVING AN ASSOCIATION BETWEEN AN IP ADDRESS AND CRIMINAL ACTIVITY.

While *amici* have no view regarding the outcome of this case, the evolving nature of internet technology and the wide range of factual scenarios in which such technologies are deployed suggest that courts should engage in a "totality of the circumstances" analysis when issuing and reviewing warrants such as the one at issue in the present

appeal. *People v. Bailey*, 2018 CO 84, ¶ 20 (quoting *Mendez v. People*, 986 P.2d 275, 280 (Colo. 1999)); *District of Columbia v. Wesby*, 583 U.S. 48, 57 (2018).

Under some circumstances, applying the "common occupation" and "suspect premises" doctrines to IP addresses, *see People v. Dhyne,* 2022 COA 122, ¶¶ 16-18, 50, may create unintended consequences mirroring the conundrum of "unfettered access" to devices as in *Coke,* ¶ 36. Instead, issuing judges and reviewing courts should consider the "totality of circumstances" in evaluating search warrants which are based upon an association between an IP address and suspected criminal activity.

A "totality of the circumstances" analysis is more capable of contextualizing the many different factual scenarios in which IP addresses might or might not be associated with criminal activity, than the doctrines relied upon by the Court of Appeals. Such an analysis is therefore better attuned to ensuring that search warrants in cases involving an association between an IP address and criminal activity respect relevant constitutional principles—especially as computer networking technology continues to evolve.

Some considerations that courts should evaluate in ensuring that such warrants meet the constitutional requirements of probable cause and particularity may include:

- The number of people and devices accessing the internet through a given IP address;
- Whether the internet connections at issue are wired or wireless;
- In the case of wireless connections, whether the wireless network is configured to be private or public;
- The range of the wireless network in question; and
- The availability of technical information that may be able to identify the kind of device or the specific device on the network implicated in criminal activity.

Amici acknowledge that the "totality of the circumstances" analysis they are proposing will not provide law enforcement, criminal defendants, and issuing and reviewing courts with bright-line rules to govern such searches. Even so, *amici* believe that the iterative application of such an analysis over time will help all participants in the criminal justice system understand the standards required to establish probable cause and particularity as networking technology continues to evolve.

Respectfully submitted and dated this 6th day of November 2023.

/s/ Vivek Krishnamurthy
Attorneys for *Amici Curiae* Professors of Law & Engineering

Vivek Krishnamurthy (Law Prof. Reg. #58996)
Sebastian Blitt (Student Attorney)
Madeline Finlayson (Student Attorney)
Sarah Misché (Student Attorney)

University of Colorado Law School Clinical Programs
Wolf Law Building | 404 UCB
2450 Kittredge Loop Drive
Boulder, Colorado 80309
(303) 492-0209
vivek.krishnamurthy@colorado.edu

Addendum

Constitution of the United States of America
Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Constitution of the State of Colorado
Article II, Section 7

The people shall be secure in their persons, papers, homes and effects, from unreasonable searches and seizures; and no warrant to search any place or seize any person or things shall issue without describing the place to be searched, or the person or thing to be seized, as near as may be, nor without probable cause, supported by oath or affirmation reduced to writing.

Certificate of Service

This is to certify that I have duly served the **Brief of Amici Curiae Law and Engineering Professors** upon all parties via the Colorado Courts e-filing system on November 6, 2023.

/s/ Vivek Krishnamurthy
Attorneys for *Amici Curiae* Professors of Law & Engineering

Vivek Krishnamurthy (Law Prof. Reg. #58996)
Sebastian Blitt (Student Attorney)
Madeline Finlayson (Student Attorney)
Sarah Misché (Student Attorney)

University of Colorado Law School Clinical Programs
Wolf Law Building | 404 UCB
2450 Kittredge Loop Drive
Boulder, CO 80309
(303) 492-0209
vivek.krishnamurthy@colorado.edu