SJC-12076

COMMONWEALTH vs. ADALBERTO MARTINEZ.

Bristol. October 6, 2016. - February 7, 2017.

Present: Gants, C.J., Botsford, Lenk, Hines, Gaziano, Lowy, & Budd, JJ.

Obscenity, Child pornography. Constitutional Law, Search and seizure. Search and Seizure, Computer. Evidence, Information stored on computer.

Complaint received and sworn to in the Fall River Division of the District Court Department on May 9, 2012.

A pretrial motion to suppress evidence was heard by Kevin J. Finnerty, J., and the case was tried before him.

The Supreme Judicial Court on its own initiative transferred the case from the Appeals Court.

Michelle A. Dame for the defendant.
Soshana E. Stern, Assistant District Attorney, for the Commonwealth.

BOTSFORD, J. The defendant, Adalberto Martinez, appeals from his conviction of possessing child pornography in violation of G. L. c. 272, § 29C. He challenges the denial of his motion

to suppress computer evidence obtained pursuant to a search warrant. The gravamen of the defendant's claim is that the police needed to do more to link the defendant to the place searched and the items seized before a warrant could validly issue. We affirm the denial of the motion to suppress and the conviction.

Background. 1. IP addresses. All computers that connect to the Internet identify each other through a unique string of numbers known as an Internet protocol address (IP address). See Internet Corporation for Assigned Names and Numbers, Beginner's Guide to Internet Protocol (IP) Addresses 2, 4 (2011) (ICANN Guide). In general, when a subscriber purchases Internet service from an Internet service provider (ISP), the ISP selects from a roster of IP addresses under its control and assigns a unique IP address to the subscriber at a particular physical address. See id. at 4, 6; United States v. Kearney, 672 F.3d 81, 89-90 & n.6 (1st Cir. 2012). See also Office of Legal Education, United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 65 (2009) (DOJ, Searching and Seizing Computers). The IP address assigned to a particular subscriber may change over time, but the ISP keeps a log of which IP address is assigned to each subscriber at any given moment in time. See Kearney, supra; DOJ, Searching and Seizing Computers, supra.

In the early days of the Internet, when a residential Internet subscriber went online using only a home computer connected to a hard-wired Internet connection, there was a very strong correlation between an IP address assigned to a subscriber and a particular computer. Now, however, many subscribers use a wireless Internet router, which allows multiple devices within the range of the router to connect to the Internet simultaneously. See United States v. McLellan, 792 F.3d 200, 213-214 (1st Cir.), cert. denied, 136 S. Ct. 494 (2015), and cases cited. To the outside world, all of these devices will share a single public IP address -- the one that the ISP has assigned to its subscriber. See id. But internally, the router will identify each connected device by the device's own identifying number in order to channel data to and from the appropriate device. See id. See also ICANN Guide, supra at 4. As a result, the correlation between an Internet subscriber's assigned IP address and any one particular Internet-enabled device may often be weaker than it once was. However, the correlation between an IP address and a physical address can still be strong, at least when the ISP has verified its assignment of a particular IP address to a subscriber at a specific physical address at a specific point in time. See DOJ, Searching and Seizing Computers, supra at 65-66; Mackey, Schoen, & Cohn, Unreliable Informants: IP Addresses, Digital Tips and

Police Raids 8-10 (Sept. 2016), available at https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_address_white_paper_0.pdf [https://perma.cc/Y42U-C5TG] (EFF, Unreliable Informants).

2. Search warrant affidavit. The affidavit in support of the contested search warrant and related materials aver the following. On March 9, 2012, State police Sergeant Michael Hill was investigating the use of "peer-to-peer" file sharing programs to possess and distribute child pornography. One such file-sharing program, Ares, allows a user to connect to another user's computer via the Internet and then download digital files that are stored locally on the other user's computer. Ares is an open-source software that any person can download for free via the Internet. There is a special version of the Ares program for law enforcement agencies that allows them to monitor and investigate individuals suspected of using Ares to share digital files of child pornography. Using the law enforcement version of Ares to download a file from another Ares user, investigators can determine (1) the user's IP address, (2) whether the user possesses and is sharing a particular file, (3) the "hash value" associated with a particular file,[1] (4) the user's Ares username, and (5) the version of Ares software that

[1] Each file shared through Ares is identified by its "hash value" -- a string of numbers that, for all practical purposes, uniquely identifies a digital file.

the user's computer is operating. Because the law enforcement version of Ares displays both the IP addresses of Ares users and the hash values of files being shared, when police identify a file as one that contains child pornography, police can determine with a high degree of confidence when that child pornography file is being shared through a specific IP address.

In this case, Hill discovered that a computer using the IP address 65.96.142.191 and displaying the username "datflypapi@Ares" was sharing suspected child pornography via the Ares network. Through an online mapping tool (several of which exist on publicly accessible Web sites), Hill determined that this IP address was likely associated with a computer in Massachusetts. The computer using this IP address was sharing a total of ten files via the network. Hill found that a majority of these files had names containing terms commonly associated with child pornography. Over approximately thirty minutes, Hill downloaded and viewed four video files from the suspect computer and concluded that these files were child pornography. While downloading the files, Hill used another program that confirmed that a computer associated with the IP address 65.96.142.191 was connected to his computer.

By conducting an Internet search, Hill determined that the IP address in question was associated with Comcast Cable (Comcast), a major cable company and ISP. Based on the above

information, the district attorney for the Berkshire district issued an administrative subpoena to Comcast asking to whom the IP address 65.96.142.191 was assigned during the thirty-minute period on March 9, 2012, during which Hill downloaded the four suspected child pornography video files from datflypapi@Ares. Comcast responded to the subpoena on March 15, 2012, and provided information that the IP address was assigned to a subscriber named "Angel Martinez" at a certain address in Fall River (apartment). Hill then referred the investigation to Detective Steven Washington of the Fall River police department. On April 2, 2012, Washington went to the apartment, which is part of a housing development. Washington discovered that Maria Avilez[2] leased the apartment. On April 3, 2012, Washington sought and received, from the Fall River Division of the District Court, a warrant to search the apartment for computers and related items connected to the suspected possession and distribution of child pornography.

3. Execution of the search warrant. Washington and two other officers executed the warrant on April 5, 2012. According to Washington's trial testimony, when the officers first knocked

[2] The search warrant and supporting affidavit identify one of the occupants of the apartment as "Maria Avilez." The trial transcript refers to her as "Maria Alvarez" or "Maria Avelez." In this opinion, we use the name on the search warrant. The search warrant affidavit also refers to Avilez as the mother of Angel Martinez. At trial, she was identified as the grandmother of both Angel Martinez and the defendant, Adalberto Martinez.

on the door of the apartment, no one answered.[3] Washington then heard someone say, "Hey, he just ran out that way," and saw a "large male" running down a side street away from the apartment. The officers eventually entered the apartment. Inside they encountered the defendant's girl friend, Ruth Pereira, holding her infant child. Both Avilez and Angel Martinez, the defendant's cousin, arrived at the apartment while officers were conducting the search, but the defendant was not present.

During the search, Washington noticed two laptop computers underneath a basket of laundry. After some initial testing (which was not described in detail in the trial record), the officers seized the two computers and brought them back to the police station.[4] Upon further inspection at the station, officers discovered five video files of child pornography on one of the defendant's laptop computers. It is not clear from the record whether any of these video files were among those observed by Hill during his Ares surveillance on March 9, 2012.

4. Procedural history. A complaint issued charging the defendant with one count of distribution of material depicting a child engaged in a sexual act, in violation of G. L. c. 272,

[3] The pretrial hearing on the defendant's motion to suppress evidence seized during the search of the apartment was nonevidentiary.

[4] The defendant's girl friend, Ruth Pereira, testified at trial that the two computers belonged to the defendant. The defendant does not challenge the accuracy of this testimony.

§ 29B (b), and one count of possession of child pornography, in violation of G. L. c. 272, § 29C. Prior to trial, the defendant moved to suppress the evidence obtained in executing the search warrant described above. He argued that the search warrant affidavit did not establish probable cause that the contraband being sought would be present in the apartment, and therefore the search violated his rights under the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights. After a hearing, a District Court judge denied the motion. The judge ruled that the affidavit and accompanying exhibits provided probable cause to believe evidence of specific criminal activity would be found at the apartment.

The defendant was tried before and convicted by a jury in the District Court on the charge of possession of child pornography; the Commonwealth filed a nolle prosequi of the distribution charge. The defendant timely appealed from his conviction, and we transferred the appeal to this court on our own motion.

Discussion. The sole issue on appeal is the validity of the search warrant issued for the apartment. Detective Washington's affidavit in support of the search warrant averred that a particular IP address was used to share child pornography and that this IP address had been assigned at the time in

question to an Internet subscriber at the specific physical address to be searched. The central question is whether these averments were sufficient to establish probable cause for the search, even though the named subscriber was neither listed as, nor confirmed to be, living in the unit, and even though police had no information before the search linking the defendant to the residence. We conclude that the affidavit in this case did establish probable cause to search the apartment for computer evidence related to the suspected possession or distribution of child pornography.

"Under the Fourth Amendment and art. 14, a search warrant may issue only on a showing of probable cause."[5] Commonwealth v.

[5] The defendant is correct that, in certain circumstances, art. 14 of the Massachusetts Declaration of Rights provides more substantive protection to criminal defendants than the Fourth Amendment to the United States Constitution. See, e.g., Commonwealth v. Rodriguez, 472 Mass. 767, 776 (2015). Here, we conclude that there was probable cause for the search warrant under both art. 14 and the Fourth Amendment. As for the Fourth Amendment, our conclusion accords with the decisions of several Federal courts that have found probable cause in similar factual settings. See, e.g., United States v. Valley, 755 F.3d 581, 587 (7th Cir.), cert. denied, 135 S. Ct. 461 (2014) (probable cause existed when investigators downloaded child pornography from IP address, then traced IP address to residence defendant shared with his mother); United States v. Vosburgh, 602 F.3d 512, 526 (3d Cir. 2010), cert. denied, 563 U.S. 905 (2011) (noting that "several 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," and so holding); United States v. Perez, 484 F.3d 735, 740 (5th Cir.), cert. denied, 552 U.S. 952 (2007) (probable cause based on information in affidavit that child pornography was viewed by

Anthony, 451 Mass. 59, 68 (2008). "The probable cause necessary to support the issuance of a search warrant does not require definitive proof of criminal activity." Id. at 69. Rather, a warrant may issue if a magistrate finds "a substantial basis on which to conclude that the articles or activity described are probably present or occurring at the place to be searched" (emphasis in original). Id. To determine whether probable cause exists, our inquiry "always begins and ends with the four corners of the affidavit." Id. at 68, quoting Commonwealth v. O'Day, 440 Mass. 296, 297 (2003). For probable cause to arise, the facts contained in an affidavit, plus the reasonable inferences that may be drawn from them, must allow the magistrate to determine that "the items sought are related to the criminal activity under investigation, and that they reasonably may be expected to be located in the place to be searched at the time the search warrant issues." Commonwealth v. McDermott, 448 Mass. 750, 767, cert. denied, 552 U.S. 910 (2007), quoting Commonwealth v. Cinelli, 389 Mass. 197, 213, cert. denied, 464 U.S. 860 (1983). See Anthony, supra at 68.

---

computer using particular IP address and that this IP address was assigned to user at specific physical address; noting that although "it was possible that the transmissions originated outside of the residence to which the IP address was assigned, it remained likely that the source of the transmissions was inside that residence"); United States v. Grant, 218 F.3d 72, 75 (1st Cir.), cert. denied, 531 U.S. 1025 (2000) (probable cause existed even discounting for possibility that someone other than Internet account registrant was using account).

"[S]earch warrant affidavits are to be interpreted in a realistic and commonsense manner," not "subjected to hypercritical analysis" (citation omitted). Id. at 69.

The probable cause inquiry in this case asks whether the facts averred in Washington's affidavit showed a sufficient nexus between the suspected criminal activity (possessing or distributing child pornography), the items sought (computers and related materials), and the place to be searched (the apartment). See McDermott, 448 Mass. at 768-769. To that end, the nexus between the suspected criminal activity, the items sought, and the place to be searched may be based on, among other things, the type of crime, the extent of the suspect's opportunity for concealment, and normal inferences about where a criminal would be likely to hide evidence of the suspected crime. See id. at 768.

Here, the affidavit described how Sergeant Hill had observed a computer associated with the IP address 65.96.142.191 that contained, and was sharing, child pornography via the Ares network. An Internet search revealed that this IP address had been issued to Comcast, the ISP. The district attorney for the Berkshire district then issued a subpoena to the ISP, which revealed that the IP address in question had been assigned during the relevant time period to a subscriber at the physical

address of the apartment.[6] The temporal and geographical links between the target IP address and the physical address to be searched provided a substantial basis for concluding that evidence sought (computers and related items) was connected to the suspected crime (possessing or sharing child pornography) and likely would be found at the specified premises (the apartment), and therefore gave rise to a sufficient nexus between the suspected criminal activity and the residence. See Commonwealth v. Augustine, 472 Mass. 448, 455 (2015); Commonwealth v. Foster, 471 Mass. 236, 241–242 (2015).

Of course, the ISP also provided a name associated with the service address and officers took subsequent steps to determine who actually lived at the apartment. In many cases, those pieces of information can serve a useful confirmatory role. But in the present case, we conclude that there was probable cause to search for evidence related to sharing child pornography based on the information police obtained through their Ares surveillance and the administrative subpoena, independent of whose name was on the Internet account or in the housing

[6] We note that the administrative subpoena is generally a more reliable method of connecting an IP address with a physical address, as compared to certain IP address mapping services. See Mackey, Stanton, Schoen, & Cohn, Electronic Frontier Foundation, Unreliable Informants: IP Addresses, Digital Tips and Police Raids 8-9 (Sept. 2016), available at https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_address_white_paper_0.pdf [https://perma.cc/Y42U-C5TG] (discussing error rates of some IP address mapping services).

development's records. The probable cause showing necessary for issuance of a search warrant is "only a fair probability that evidence of such a crime would be found in particular locations," not "a prima facie showing that the defendant possessed child pornography." Anthony, 451 Mass. at 72. Police met that threshold here.

The defendant advances, in essence, three arguments about why investigators needed to do more to establish probable cause. We address each in turn.

First, he points out that before applying for the search warrant, the police were unable to verify that the subscriber named by the ISP -- Angel Martinez -- lived at the apartment, and also were unable to rule out the possibility that someone other than the named subscriber was responsible for using the IP address assigned to the apartment at the time in question. Therefore, the defendant argues, it was possible that a new (and innocent) person had moved into the apartment while Angel Martinez, living at a different address altogether, continued to pay the Internet bill, or that a new occupant merely took over the Internet payments without changing the name on the account. To support his position, the defendant cites several cases in which investigators obtained more information linking an individual suspect to a specific physical address before applying for a search warrant. See, e.g., United States v.

Elbe, 774 F.3d 885, 887–888 (6th Cir. 2014), cert. denied, 135 S. Ct. 1573 (2015) (agents observed person matching child pornography suspect's driver's license photograph sitting on porch of target residence); United States v. Stults, 575 F.3d 834, 838 (8th Cir. 2009), cert. denied, 559 U.S. 915 (2010) (public records check using LexisNexis, postal service mail delivery check, and motor vehicle registration check all confirmed that named Internet subscriber actually resided at target residence).

It is true that investigators had no direct information that Angel Martinez personally had used, was using, or would ever use the IP address in question. However, in this particular case, the name of the Internet account holder did not defeat probable cause. See Commonwealth v. Molina, 476 Mass. , (2017). The question before the magistrate was whether the apartment located at a certain address likely contained evidence of criminal activity -- period. The question was not whether that address likely contained evidence of criminal activity on the part of Angel Martinez (or on the part of Avilez for that matter).

To that end, Detective Washington's supporting search warrant affidavit spelled out a relatively direct link between (1) the downloading and sharing of child pornography video files, (2) a specific IP address, and (3) a specific physical

address to which that IP address had been assigned. From a technological standpoint, an IP address can be assigned to only one service address at any given point in time. See United States v. Vosburgh, 602 F.3d 512, 527 & n.14 (3d Cir. 2010), cert. denied, 563 U.S. 905 (2011), and cases cited (noting "unique nature of the IP address assigned" to defendant on particular date made Internet activity on that date "fairly traceable" to specific ISP account and associated physical address); DOJ, Searching and Seizing Computers, supra at 65. Taken together, these facts gave rise to a reasonable inference that evidence related to possession or distribution of child pornography via the Internet likely would be found at the apartment -- the one place, according to the ISP's records, to which the IP address in question was assigned during the relevant time period.

Once this nexus was established, the name of the account holder was essentially incidental. See Molina, 476 Mass. at . Although information showing that the named subscriber was also the person suspected of possessing or sharing the child pornography might have increased the likelihood that the sought-after evidence would be located at the service address, the lack of such information does not necessarily defeat probable cause. See United States v. Grant, 218 F.3d 72, 75 (1st Cir.), cert. denied, 531 U.S. 1025 (2000). This is so precisely because an

IP address can be assigned to only one service address at any given time -- regardless of whose name is on the account.[7] See Vosburgh, 602 F.3d at 527 & n.14.

Second, the defendant points out that investigators did not determine whether the Internet connection at the apartment used a wireless router and, if so, whether the wireless network required a password. This left open the possibility that someone other than the subscriber, located at a different physical address, was "joyriding" on an unsecured wireless network based out of the apartment. See Snow, Accessing the Internet Through the Neighbor's Wireless Internet Connection: Physical Trespass in Virtual Reality, 84 Neb. L. Rev. 1226, 1227-1229 (2006). The defendant argues that this concern is especially acute in the present case because investigators knew that the apartment was part of a housing development, in which multiple residences were in close proximity to the target physical address.

The defendant's argument is misdirected. A showing of probable cause to search a place (as opposed to arrest a person)

---

[7] The defendant does not now claim that the information in the police affidavit had become stale. The defendant's motion to suppress did include a passing reference to staleness. However, this theory was not advanced at the suppression motion hearing, and the defendant's brief does not make such an argument. Any staleness issue, therefore, is waived. See Commonwealth v. Wood, 389 Mass. 552, 554 n.3 (1983), citing Mass. R. A. P. 16 (a) (4), as amended, 367 Mass. 919 (1975).

need not identify a specific criminal suspect -- although frequently it does. See Zurcher v. Stanford Daily, 436 U.S. 547, 555-557 & n.6 (1978). See also Molina, 476 Mass. at . Indeed, "[t]he critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought." Zurcher, supra at 556. In other words, police need only demonstrate a sufficient nexus between the criminal activity under investigation, the items sought, and a place to be searched where the items may reasonably be expected to be located -- independent of whether they have identified a specific criminal suspect.[8] See McDermott, 448 Mass. at 767-768; O'Day, 440 Mass. at 302-304. Certainly police may have an easier time demonstrating a sufficient nexus if they can link a specific suspect (e.g., the named Internet account holder) to

[8] To this point, the prosecutor and Detective Steven Washington had the following colloquy at trial:

> Q.: "Now when you execute a warrant like this . . . are you conducting . . . [the search] for a person or for a device?"
>
> A.: "A device."
>
> Q.: "Okay. And why is that?"
>
> A.: "Because I have no clue who is behind that device."

the criminal activity. However, such a link is not always required.

The search warrant affidavit in this case demonstrated that child pornography was being shared via the Internet from a specific IP address. This IP address, in turn, had been assigned to a specific physical address during the time when the child pornography was being shared. These facts provided a substantial basis from which to conclude that evidence of downloading and sharing child pornography via the Internet would be located at the apartment, even if it turned out that an unauthorized user was "joyriding" using the targeted IP address. See Augustine, 472 Mass. at 455; Commonwealth v. Escalera, 462 Mass. 636, 645 (2012), quoting 2 W.R. LaFave, Search and Seizure § 3.7(d), at 420-421 (4th ed. 2004) (police do not need to provide definitive proof that evidence of suspected criminal activity will be located at targeted residence, only facts supporting reasonable inference that such evidence "probably" would be located there). See also Grant, 218 F.3d at 75 (even discounting for possibility that individual other than subscriber may have been using account, there was fair probability that subscriber was user and that evidence of user's illegal activities would be found in subscriber's home).[9]

[9] This close nexus also distinguishes a case like Commonwealth v. Kaupp, 453 Mass. 102 (2009). In that case, we

The defendant is correct, from a technological standpoint, that if an Internet subscriber at the apartment set up an unsecured wireless Internet network, a computer outside of this physical address (in a neighboring unit, perhaps) could have used the targeted IP address to access the Internet and share child pornography.[10] This point misses the mark, because

---

held that police lacked probable cause to search a specific computer for evidence of child pornography. Id. at 113-114. However, in the Kaupp case, there was no indication that a specific IP address had been used to download or share child pornography. Instead, police essentially relied on the fact that the targeted computer may have shared another, nonpornographic file with a computer that did contain child pornography, and that these two computers were connected in a way that made it possible for them to share other files. See id. at 111-112. The nexus in this case -- where an officer directly observed child pornography being transmitted through the targeted IP address, which could only be assigned to one physical address at the time in question -- is substantially stronger.

[10] Notably, there was no evidence, either at the suppression stage or at trial, that the apartment was home to an unsecured wireless Internet connection or that anyone other than the defendant used the Internet connection there. Nor was there any evidence that the defendant did not connect his laptop computers to the Internet through the IP address assigned to the apartment. However, even if we accept the defendant's hypothetical scenario of "joyriding," and it turned out that none of the defendant's devices contained child pornography, police still would have had probable cause to seize and search any Internet modems or routers in order to determine which devices were connected to the targeted IP address at the time when police witnessed child pornography being shared via the targeted IP address. See United States v. Stanley, 753 F.3d 114, 115-117 (3d Cir.), cert. denied, 135 S. Ct. 507 (2014) (describing how wireless Internet router keeps log of devices that have connected to it). If those devices, or other information, then led police to a device at a different physical address from the one linked to the IP address through the ISP's

probable cause does not require investigators to "establish to a certainty that the items to be seized will be found in the specified location," nor does it require them to "exclude any and all possibility that the items might be found elsewhere." Anthony, 451 Mass. at 70, quoting Commonwealth v. Harmon, 63 Mass. App. Ct. 456, 461 (2005).

Finally, the defendant argues that, in a case like this, probable cause cannot arise until police show one of three things: (1) that the target IP address has not been linked to a wireless Internet service; (2) that the target IP address is linked to a wireless Internet service, but it is a secure connection requiring a password; or (3) that no one outside the target physical address could be accessing the network. The defendant urges that, without these showings, the likelihood of someone outside the target physical address using the target IP address is substantial enough to defeat probable cause. By and large, these proposals simply restate the defendant's arguments

---

records, police likely would have needed another warrant. Cf. United States v. Voustianiouk, 685 F.3d 206, 213-214 (2d Cir. 2012) (where police omitted target's name from application for warrant to search specific apartment, second warrant was required once it became clear target lived in different apartment); United States v. Greathouse, 297 F. Supp. 2d 1264, 1274–1275 (D. Or. 2003) (second warrant required when it became clear to officers executing warrant that target resided in rented room within house). But, as illustrated above, that scenario is several steps removed from what occurred here, where police quickly located two laptop computers that belonged to the defendant, one of which contained five video files of child pornography.

urging that the police, in order to show probable cause, should have been required to rule out the possibility that persons outside of the apartment may have been "joyriding" on the IP address assigned to that location at the time in question. To the extent that is the case, we reject these proposals for the reasons already mentioned.

Moreover, as the Commonwealth points out, it is not clear whether it would be technologically feasible for investigators to do what the defendant asks. With respect to the first proposal, there is nothing in the record showing that a third party (like an ISP, for instance) would be able to determine whether a subscriber's connection to the Internet is through a hard-wired or wireless connection at any given point in time. With respect to the second, in the case of a subscriber who uses a wireless router, it is not clear how investigators would be able to ascertain whether the network is password-protected without first learning the name of that subscriber's wireless network. And regarding the third proposal, even assuming investigators knew that a target IP address was associated with an unprotected wireless network that had been accessed by devices not belonging to the subscriber, these considerations would not necessarily change the fact that, given the Ares surveillance conducted in this case, there remained a fair probability that any computers located at the apartment would

contain evidence related to the possession or distribution of child pornography. See United States v. Stanley, 753 F.3d 114, 115-117 (3d Cir.), cert. denied, 135 S. Ct. 507 (2014) (based on file-sharing surveillance similar to that conducted in this case, police obtained valid search warrant for home linked to target IP address; only after police found no evidence of child pornography there and learned, in course of their search, that home deployed wireless Internet network that was not password-protected did they take subsequent steps to locate true suspect); United States v. Perez, 484 F.3d 735, 740 (5th Cir.), cert. denied, 552 U.S. 952 (2007) (although possible that Internet transmissions originated outside of residence to which IP address was assigned, it remained likely that source of transmissions was inside that residence); Grant, 218 F.3d at 75 (similar); United States v. Carter, 549 F. Supp. 2d 1257, 1268–1269 (D. Nev. 2008) (similar). The defendant's proposals merely illustrate that different hypothetical scenarios could lead to a different conclusion regarding probable cause. But those potentialities do not necessarily defeat probable cause, especially when they lack any factual underpinning. See Anthony, 451 Mass. at 70 (discussing nexus requirement). Instead, the fundamental question is whether there was a substantial basis from which to conclude that the items described in the application were probably present at the place

to be searched. See id. at 69. For all of these reasons, we affirm the denial of the defendant's motion to suppress.[11]

We end with a cautionary note. Our decision today should not be read to mean that probable cause always exists any time investigators link illegal computer activity to an IP address and then link that IP address to a physical address. For one, police should (as they did in this case) connect the IP address with a physical address through a reliable method, such as an administrative subpoena to the ISP, rather than relying solely on a potentially unreliable method, such as certain IP address mapping services. See note 6, supra. Additionally, technologies that apparently were not at issue in this case may further erode the connection between an IP address and a physical address. See EFF, Unreliable Informants, supra at 10-11 (discussing how Tor exit relays, virtual private networks, and proxy server connections can mask originating IP addresses through use of one or more intermediary IP addresses); Vosburgh, 602 F.3d at 527 n.14 (discussing "possibility of mischief and mistake with IP addresses" such that, in some cases, "value of

[11] The defendant does not challenge the reasonableness or scope of the search of his digital files once police had seized his computers, nor does he raise the related issue whether courts should require police to develop minimization techniques to govern the execution of a digital search. Accordingly, we need not address those issues here. However, in an appropriate case, we would consider whether to require some type of digital search protocol. See Commonwealth v. Molina, 476 Mass. , (2017).

that IP address for probable cause purposes may be greatly diminished, if not reduced to zero").

At the very least, certain cases may require police to disclose in a search warrant affidavit the possibility that one of these technologies is, or may be, in play based on facts known or reasonably knowable to investigators at the time. See EFF, Unreliable Informants, supra at 18. If such technologies become more common, it is entirely possible that we would require police to proceed in multiple steps, obtaining subpoenas related to each intermediary IP address or warrants to search each location hosting those IP addresses. Alternatively, some cases may require the police to examine forensically a wireless router to determine which devices were connected to it, and when, before they search particular computers. See Stanley, 753 F.3d at 115-117 (describing police investigation based on information obtained by examining innocent Internet user's unprotected wireless Internet router that had been "hijacked" by neighbor-defendant to share child pornography).

Such possibilities demonstrate why the probable cause analysis rarely, if ever, lends itself to bright-line rules. See Escalera, 462 Mass. at 643 ("No bright-line rule can establish whether there is a nexus" between suspected criminal activity and defendant's home). This is especially so when, as here, the analysis hinges on fluid and rapidly changing

technologies. Cf. Commonwealth v. Dorelas, 473 Mass. 496, 502 & n.11 (2016) (noting that "what might have been an appropriate limitation [on searches] in the physical world becomes a limitation without consequence in the virtual one"); id. at 505 (Lenk, J., dissenting) (transposing protections of art. 14 and Fourth Amendment to digital contexts "is an ongoing and challenging task"); Commonwealth v. Phifer, 463 Mass. 790, 797 (2012) (noting that developments in cellular telephone technology "present novel and important questions about the relationship between the modern doctrine of search incident to arrest and individual privacy rights").

Conclusion. The order denying the motion to suppress and the defendant's conviction are affirmed.

So ordered.