SJC-12829

COMMONWEALTH vs. ROBERT GUASTUCCI.

Middlesex. March 5, 2020. - October 14, 2020.

Present: Gants, C.J., Lenk, Gaziano, Lowy, Budd, Cypher, & Kafker, JJ.[1]

Obscenity, Child pornography. Constitutional Law, Search and seizure, Probable cause. Probable Cause. Search and Seizure, Computer, Probable cause, Affidavit. Evidence, Information stored on computer. Practice, Criminal, Motion to suppress.

Indictments found and returned in the Superior Court Department on February 15, 2018.

A pretrial motion to suppress evidence was heard by John T. Lu, J., and a conditional plea of guilty was accepted by him.

The Supreme Judicial Court granted an application for direct appellate review.

Benjamin L. Falkner for the defendant.
Gabriel Pell, Assistant District Attorney, for the Commonwealth.

[1] Chief Justice Gants participated in the deliberation on this case prior to his death.

GAZIANO, J. On March 15, 2017, an unknown computer user uploaded an image of child pornography to an Internet-based communication service that is designed to share files and "chat" with others. After receiving a tip from the National Center for Missing and Exploited Children (NCMEC), police tracked the specific computer address by which the device had connected to the Internet to the defendant's house in Tyngsboro, and an account owned by his wife. Seven months after the alleged illegal activity, on October 18, 2017, a State police trooper obtained a warrant authorizing a search of all computer systems and digital storage devices located within the residence for evidence of child pornography. Following execution of the search warrant, the defendant's laptop computer and a "flash" drive were seized; the defendant subsequently was indicted on two counts of possession of child pornography, in violation of G. L. c. 272, § 29C, as a result of images found on these devices.

At issue in this appeal is whether the information in the search warrant affidavit was too stale to establish probable cause to believe that evidence of child pornography would be found on computers or digital storage devices at the time of the search, seven months after the Internet activity with one specific image. A Superior Court judge denied the motion to suppress after finding that the seven-month period was "less

than ideal, but . . . a tolerable amount of delay." The defendant subsequently entered a conditional guilty plea to both charges, see Commonwealth v. Gomez, 480 Mass. 240, 252 (2018), and we allowed his petition for direct appellate review. Because we conclude that there was sufficient evidence for a magistrate to have found probable cause, we affirm.

1. Background. a. Investigation and warrant application. On October 18, 2017, State police Trooper Christopher MacDonald applied for a warrant to search computers and digital storage devices located within a single-family house in Tyngsboro. In support of the warrant application, McDonald submitted a ten-page affidavit and an attached exhibit. The exhibit described, in general terms, the investigation of child pornography that has been distributed over the Internet and stored in a suspect's computer. The affidavit and exhibit then stated the following.

On March 16, 2017, electronic service provider Skype.com (Skype) filed a report with NCMEC of a suspected incident of possession or distribution of child pornography.[2] Skype is a

[2] The National Center for Missing and Exploited Children (NCMEC), among other functions, operates a "CyberTip line" that the public may use to report suspected instances of Internet-related child exploitation. Pursuant to 18 U.S.C. § 2258A(a)(1)(A), Internet service providers are required to report suspected child pornography to NCMEC "as soon as reasonably possible." In its role as a clearing house for this type information, NCMEC forwards these tips to Federal and State law enforcement agencies. See 18 U.S.C. § 2258A(c)(1)-(3).

Web-based application that provides its customers with video communication and voice call services, as well as "chat" services where typed messages are exchanged interactively. Skype users also may use the platform to exchange digital images and video files. According to the information reported by Skype, a computer user with a "screen name" of "live: boullett_1" at a particular Internet Service Protocol (IP) address uploaded a digital image believed to be child pornography on March 15, 2017. At a date not specified in the affidavit, NCMEC forwarded the information contained in the tip to the State police computer crimes unit.

On May 5, 2017, pursuant to an administrative subpoena issued by the Massachusetts Attorney General's Office, the internet service provider (ISP) provided records for its subscriber at that IP address. The ISP identified the subscriber, as of March 15, 2017, as the defendant's spouse, with a service address in Tyngsboro. The Internet account, which had been created in August of 2007, listed three user names; none of these matched the Skype screen name "live: boullett_1" that had been used to upload the image.

On September 27, 2017, McDonald viewed the digital image uploaded to Skype and confirmed that it depicted child pornography. That day, he queried the registry of motor vehicles for vehicles and driver's licenses registered at the

street address in Tyngsboro. He found three listed drivers: the defendant, his spouse, and their child. On October 11, 2017, MacDonald conducted surveillance of the single-family home and "was unable to locate any open unprotected wireless networks within the vicinity of the residence."

In addition to the facts involving this investigation, MacDonald's affidavit included generalized information about possession of child pornography. He averred that "[t]hose who have possessed and/or disseminated child pornography have an interest or preference in the sexual activity of children" and are "likely to keep secreted, but readily at hand, sexually explicit visual images depicting children. . . . These depictions tend to be extremely important to such individuals and are likely to remain in the possession of or under control of such an individual for extensive time periods."

He further averred that, in the event an individual with an interest in child pornography were to delete a file, it could be possible to recover that evidence from the computer's hard drive or temporary storage "months or years" after it had been deleted. The ability to recover deleted files depends upon many factors, including whether temporary files have been overwritten by new data; whether the hard drive has been damaged; and whether the computer user effectively encrypted the data.

The search warrant was issued, and police executed the warrant on October 19, 2017. The search yielded a laptop computer and a flash drive, both owned by the defendant, which contained images of child pornography.

b. Prior proceedings. A grand jury returned indictments charging the defendant with two counts of possession of child pornography, in violation of G. L. c. 272, § 29C. The defendant moved to suppress the evidence seized from the laptop computer and the flash drive on the ground that the affidavit failed to establish probable cause to search his home because it was based on stale information. A Superior Court judge denied the motion. The judge endorsed the motion as follows: "[A]fter hearing this motion is denied because an uploader on this online platform is in a different position than a downloader or uploader on platforms like icloud or Dropbox, March to October is less than ideal but is a tolerable amount of delay and digital files are often kept on computers for years. Also, the appellate case[s] point toward this result."

On November 13, 2018, with the Commonwealth's assent (and with the judge's acceptance), the defendant tendered a conditional guilty plea to both counts of possession of child pornography. He then filed a notice of appeal, and we allowed his motion for direct appellate review.

2. Discussion. Under the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights, a search warrant may issue upon a showing of probable cause. Commonwealth v. Anthony, 451 Mass. 59, 68 (2008). "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" (quotations and citation omitted). Commonwealth v. Martinez, 476 Mass. 410, 415 (2017). See Commonwealth v. Long, 482 Mass. 804, 809 (2019) (probable cause means substantial basis to believe evidence of criminal activity may reasonably be expected to be located in place searched "at the time the search warrant issues" [citation omitted]). "Facts asserted in the affidavit must be closely related in time to the issuance of the warrant in order to justify a finding of probable cause . . . ." Commonwealth v. Connolly, 454 Mass. 808, 814 (2009).

"Whether a search warrant is supported by probable cause is a question of law that we review de novo" (quotations and citation omitted). Commonwealth v. Vasquez, 482 Mass. 850, 866 (2019). Review of a probable cause determination is limited to the four corners of the warrant affidavit and any attachments

thereto. Commonwealth v. Perkins, 478 Mass. 97, 102 (2017). In determining whether probable cause exists, "we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men [and women], not legal technicians, act." Commonwealth v. Hason, 387 Mass. 169, 174 (1982), quoting Brinegar v. United States, 338 U.S. 160, 175 (1949). Thus, we view consider the statements in the warrant affidavit in a "commonsense manner," Commonwealth v. O'Day, 440 Mass. 296, 299 n.4 (2003), and consider the warrant affidavit "as a whole, without overly parsing or severing it, or subjecting it to hypercritical analysis" (quotations and citation omitted). Perkins, supra.

In addition, we are mindful that the probable cause inquiry is "not a high bar" (citation omitted), District of Columbia v. Wesby, 138 S. Ct. 577, 586 (2018), and that probable cause "does not require definitive proof of criminal activity," Anthony, 451 Mass. at 69. "And officers need not 'rule out a suspect's innocent explanation for suspicious facts' to obtain a warrant" (citation omitted). United States v. Chavez, 423 F. Supp. 3d 194, 205 (W.D.N.C. 2019).

The defendant does not dispute that the image viewed by police constituted child pornography or that it was uploaded from a computer at his house on the date alleged. Moreover, the

defendant does not contest that the statements in the warrant affidavit would be sufficient to establish probable cause that the image was uploaded from his computer to the Skype service. Nor does he claim that someone else accessed his computer and uploaded the image. Thus, the primary issue we must address is whether the passage of seven months between the alleged upload and the application for a search warrant rendered the warrant so stale that it lacked probable cause.

The defendant argues that the upload of a single image of child pornography is not enough, standing alone, to justify issuing a warrant to search his computer seven months later. He contends that there was nothing in the search warrant affidavit to suggest that the individual who uploaded the image was a collector of child pornography, such that the image would be likely to be retained on the laptop rather than being deleted at some point over a fairly lengthy period of time. The Commonwealth responds that, to the contrary, because the target of the search warrant deliberately uploaded an image of child pornography to Skype, a service which is designed for online conversations, chats, and sharing of files, there was probable cause to believe that the individual who uploaded the image "was interested in [child pornography] enough to retain the uploaded file." While the delay of seven months may be at the outer limit in these circumstances, we conclude, as did the motion

judge, that the information in the warrant affidavit was not stale when the warrant was filed.

Because of the highly fact-intensive nature of the inquiry, it is not possible to formulate a bright-line test for staleness. See Commonwealth v. Atchue, 393 Mass. 343, 349 (1984), quoting Sgro v. United States, 287 U.S. 206, 211 (1932) (timeliness of facts is "determined by the circumstances of each case"). See also Connolly, 454 Mass. at 814, citing Commonwealth v. Cruz, 430 Mass. 838, 843 (2000). We typically measure the timeliness of information supporting a search warrant by considering two factors: (1) the nature of the criminal activity under investigation; and (2) the nature of the item to be seized. Commonwealth v. Matias, 440 Mass. 787, 792-793 (2004); Cruz, supra.

As to the nature of the criminal activity under investigation, with crimes such as possession of narcotics, which are "readily consumed or distributed, . . . probable cause to search for them rapidly dwindles with the passage of time," and an affidavit concerning a tip about a single drug transaction that took place several months earlier would not serve to establish probable cause (quotations and citation omitted). See Matias, 440 Mass. at 792-793. See also Commonwealth v. Reddington, 395 Mass. 315, 322-323 (1985). Where an affidavit contains information indicating ongoing or

protracted criminal activity, however, the question is different, and "time is of less significance" (citation omitted). Commonwealth v. Vynorius, 369 Mass. 17, 25 (1975). See, e.g., Commonwealth v. Alvarez, 422 Mass. 198, 205 (1996) (affiant observed series of drug transactions at suspect's apartment, including transaction one and one-half weeks before seeking warrant, and individual who said he had purchased drugs from suspect the previous day was arrested on day before warrant affidavit was filed containing that information); Connolly, 454 Mass. at 817 (information was not stale where defendant was said to engage in repeated drug sales); Commonwealth v. Murphy, 95 Mass. App. Ct. 504, 510-511 (2019) (affidavit provided "powerful" evidence of ongoing theft ring).

With respect to the second factor, the nature of the item to be seized, the inquiry is related and also proceeds along two distinct lines. Information concerning an item that is perishable, readily disposable, or transferrable might not establish probable cause even a few days later. See, e.g., Commonwealth v. Wade, 64 Mass. App. Ct. 648, 651-652 (2005) (information from confidential informant that he had been purchasing cocaine from suspect who was sitting in his vehicle, and last had done so five days previously, did not establish probable cause that drugs would still be in vehicle five days later); Commonwealth v. Rodriguez, 49 Mass. App. Ct. 664, 669

(2000) (information about single instance of possession three days before issuance of warrant, without more, might not have established probable cause).

On the other hand, an item that is durable, of enduring use to its holder, and not inherently incriminating might reasonably be found in the same location several weeks later. See Commonwealth v. Gray, 465 Mass. 330, 346-347 (2013); Matias, 440 Mass. at 792-793; Commonwealth v. Burt, 393 Mass. 703, 716 (1985). See e.g., Commonwealth v. Beliard, 443 Mass. 79, 84-85 (2004) (six week old information concerning firearm was not stale where "there was no evidence that the weapons sought by the warrant had been used in any other crime, or that the defendant . . . knew that the weapons had been identified to the police thereby stripping them of their continued utility"); Commonwealth v. Blye, 5 Mass. App. Ct. 817, 818 (1977) (seemingly innocuous stolen household goods were likely to be retained for longer periods of time).[3]

---

[3] Of course, that an object is durable and useful alone is not sufficient to infer that information in the warrant is not stale. This, again, is a context-specific inquiry dependent on all the circumstances set forth in the affidavit. See, e.g., Commonwealth v. Hart, 95 Mass. App. Ct. 165, 168 (2019) (confidential informant's tip that, sixty days before application for warrant, defendant had kept semiautomatic weapon on floor in bedroom, without more, was stale, even though firearms are durable and "not likely to be consumed or destroyed" [citation omitted]). Contrast Commonwealth v. James, 424 Mass. 770, 778-779 (1997) (affidavit indicating knives had been used in recent crimes and routinely were carried by

In addition, the timeliness of the information in a search warrant depends on the ability of the police to examine an item and to detect relevant evidence of the commission of a crime at a prior time. Something that is inherently incriminating, in some circumstances, might establish probable cause well after the commission of the crime. See United States v. Contreras, 905 F.3d 853, 858-859 (5th Cir. 2018) (discussing forensic computer analysis of deleted child pornography files). Cf. Commonwealth v. Tavares, 484 Mass. 650, 652 (2020) (twelve years after murder police recovered evidence of blood stains on floor boards); Commonwealth v. Keown, 478 Mass. 232, 235-236 (2017) (police searched defendant's computer one year after spouse's death and recovered search queries "antifreeze death human" and "poison recipe").

To our knowledge, no reported Massachusetts appellate decisions have addressed the issue of staleness in the context of a search for evidence of child pornography. Courts in other jurisdictions, however, have observed that "the determination of staleness in investigations involving child pornography is unique" (citation omitted). United States v. Raymonda, 780 F.3d 105, 114 (2nd Cir. 2015). This observation is based on the

---

particular suspects was not stale eighteen days after crimes took place, where knives were to be expected to be kept at home and were not inherently incriminating).

belief that individuals who are interested in child pornography are likely to collect and retain such images in the privacy of their own homes. See United States v. Irving, 452 F.3d 110, 125 (2d Cir. 2006) (because "images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes," evidence that such persons possessed child pornography in past supports reasonable inference that they retain those images -- or have obtained new ones -- in present [citation omitted]). See also United States v. Vosburgh, 602 F.3d 512, 528 (3d Cir. 2010) (collectors of child pornography are unlikely quickly to discard images of child pornography because of difficulty and risk involved in obtaining them); United States v. Frechette, 583 F.3d 374, 378 (6th Cir. 2009) (possession of child pornography is not typically "a fleeting crime"); United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008) (customers of child pornography sites do not quickly dispose of their cache). Accordingly, the same time limitations that have been applied to "more fleeting crimes do not control the staleness inquiry for child pornography" (citation omitted). Frechette, supra.

This does not mean that a person accused of possessing or disseminating child pornography is, in effect, precluded from challenging a search warrant on the grounds of staleness because of a de facto presumption. Nor does it suggest that the

government is not bound by the requirements of the Fourth Amendment and art. 14 when seeking evidence related to allegations of possession of child pornography. Every investigation, including the possession and distribution of child pornography, has a shelf life. See Vosburgh, 602 F.3d at 529 ("We do not hold, of course, that information concerning child pornography crimes can never grow stale"). The United States Court of Appeals for the Second Circuit is one of the few appellate courts to have examined the question of the collector inference in search warrants seeking evidence of child pornography, and to have developed a more nuanced analysis. The court has explained, "Crucially, however, the value of that inference [that an individual who is interested in child pornography will retain images of child pornography for lengthy periods of time] in any given case depends on the preliminary finding that the suspect is a person 'interested in' images of child pornography." Raymonda, 780 F.3d at 114. See United States v. Falso, 544 F.3d 110, 124 (2d Cir. 2008) (generalized allegations about propensity of collectors of child pornography to hoard images is relevant to probable cause determination only if there is indication in affidavit that suspect was inclined to do so); United States v. Coreas, 419 F.3d 151, 156 (2d Cir. 2005) (alleged child pornographer's proclivities are relevant only if there is probable cause to believe that suspect is

collector of child pornography). We are persuaded that this distinction is critical and adopt this important qualification on the inferences that can be drawn in cases involving child pornography with respect to the length of time that an image containing child pornography is likely to be retained in an individual's computer or other electronic device.

We therefore must consider what constitutes evidence of an "interest in" child pornography sufficient to trigger an inference that the target of a search warrant is a collector and likely to retain such images, adequate to establish that a search warrant affidavit is not stale. As the United States Court of Appeals for the Second Circuit discussed, there are several factors that could support a reasonable inference that a suspect is a collector of child pornography: an admission or other evidence identifying the individual as a pedophile; paid subscriptions to child pornography sites or participation in peer to peer file sharing; and a past history of possessing or receiving child pornography. Raymonda, 780 F.3d 105 at 114-115, and cases cited. In addition, in some circumstances, a reasonable inference that a suspect is "interested in" child pornography might be drawn based on a single incident of possession or receipt of child pornography where, for example, the images were obtained through "a series of sufficiently complicated steps" suggesting a "willful intention to view the

files," or where the suspect redistributed the file to others. See id. at 115.

Thus, an inference that an individual is a collector of child pornography "proceed[s] from circumstances suggesting that [the suspect] accessed those images willfully and deliberately, actively seeking them out to satisfy a preexisting predilection." Id. Importantly, it excludes circumstances, even involving multiple images, where "the suspect's brush with child pornography was a purely negligent or inadvertent encounter, the residue of which was long ago expunged." Id. In Raymonda, for example, the search warrant affidavit alleged that, nine months earlier, a computer user at a specified IP address associated with the defendant's home accessed seventy-six thumbnail images of child pornography over a period of seventeen seconds. Id. at 117 & n.4, 120. The user did not download the images, or even click on the thumbnails to open them and view full-sized images. Id. at 117. The court concluded that there was not probable cause the images would still be on the computer because "[i]t was necessary to show that [the suspect] accessed [child pornography] in circumstances sufficiently deliberate or willful to suggest that he was an intentional 'collector' of child pornography, likely to hoard those images -- or acquire new ones -- long after any automatic traces of that initial incident had cleared." Id. See Falso,

544 F.3d at 121 (no probable cause where affidavit was inconclusive as to whether suspect actually gained access to child pornography website and there was no indication that he viewed or downloaded images).

Here, the defendant contends that the affidavit did not establish any "propensity-raising circumstances" so as to trigger an inference that he would have stored images of child pornography in his computer for seven months. As the defendant asserts, the affidavit does not allege that the defendant is an admitted or known pedophile, paid for access to child pornography, had a history of possessing or receiving pornographic images, or used sufficiently complicated steps to access the image in question. Nonetheless, we do not agree with the defendant's contention that there was no information in the affidavit suggesting that the person who uploaded the image redistributed that file to another person.[4] To the contrary, the affidavit alleged that the computer user, who had a Skype account and used the screen name "live: boullett_1," uploaded an

[4] The defendant also argues that the affidavit "offered no information or evidence from which the magistrate could have inferred that the particular computer or device from which the photograph was uploaded still existed." As more time passes between the upload and the search, he argues, it becomes more likely that the computer was replaced with a newer model. While, as time goes on, it is indeed more likely that a computer or other electronic device will have been replaced, seven months is not outside the realm of probability.

image of child pornography to an Internet chat, talk, and file-share service. As the motion judge noted, the use of Skype, a service that is designed for communication and file sharing, was significant, and is substantively different from, potentially inadvertently, storing (technically, "uploading")[5] a file to a cloud storage service such as "iCloud" or "Dropbox."

Given the facts as asserted in the warrant affidavit, which would have required multiple, intentional steps to place the image in a file-sharing service, it would have been unlikely that the suspect negligently or inadvertently stumbled upon the

---

[5] The key to the distinction lies in the degree of intentionality demonstrated by the user, which may depend on the software used. For certain software, as here, the inference that an upload implies intentional possession may be warranted. See United States v. Bynum, 604 F.3d 161, 166 (4th Cir. 2010). The advent of cloud computing, however, cautions against applying this inference blindly. See Riley v. California, 573 U.S. 373, 397 (2014) ("Cell phone users often may not know whether particular information is stored on the device or in the cloud"). A computer user who, intentionally or inadvertently, places a file in a cloud storage service may have intentionally acquired that file and stored it on his or her computer, or may have inadvertently saved it to cloud storage through browsing an innocuous webpage. See United States v. Bosyk, 933 F.3d 319, 346 (4th Cir. 2019) (Wynn, J., dissenting). "Cloud" services often automatically back up data with no intentional action by the user. See Comment, Child Pornography Statutes and the Cloud: Updating Judicial Interpretations for New Technologies, 57 Hous. L. Rev. 727, 748 (2020) ("If a device uploads or backs up visual depictions by default, it is not clear that the user 'knowingly' transported the visual depictions"). See also Williams vs. Apple, Inc., U.S. Dist. Ct., No. 19-CV-04700, slip op. at 2 (N.D. Cal. Mar. 27, 2020) (quoting Apple terms of service: "When iCloud is enabled, your content will be automatically sent to and stored by Apple"). See, generally, Svenson, Backup in the Modern Law Firm, 94 Mich. B.J. 54 (2015).

image and, "horrified by what he saw," promptly closed the window and deleted it. Contrast Raymonda, 780 F.3d 105 at 117. Therefore, on the facts asserted in the warrant affidavit here, it was reasonable for the magistrate to infer that the computer user "live: boullett_1" possessed a digital image of child pornography, intentionally accessed this image, and distributed it to another person by uploading the file to Skype. Compare People v. Donath, 357 Ill. App. 3d 57, 67 (2005) ("Uploading is sending something from your computer 'up' to someone else's computer. . . . Because the defendant uploaded and distributed the images, it is reasonable to infer that defendant possessed [child pornography] somewhere in his home, either on his computer or some electronic media storage device"). See also United States v. Schesso, 730 F.3d 1040, 1045 & n.2 (9th Cir. 2013) (act of uploading child pornography to file-sharing network, distinguished from "onetime accidental download or inadvertent receipt" of image, connected defendant to profile of collector of child pornography); United States v. Bynum, 604 F.3d 161, 165 (4th Cir. 2010) (probable cause to search existed based on allegation individual uploaded suspected child pornography to Internet).[6]

[6] The defendant based his argument in this court on Fourth Amendment and art. 14 grounds. As the defendant points out, in general, art. 14 provides "more substantive protection to criminal defendants than does the Fourth Amendment in the

The defendant's primary argument before the motion judge was that suppression was required based on the reasoning of the United States Court of Appeals in Raymonda, 780 F.3d 105 at 114-117. Because the defendant did not raise the propensity issue before the motion judge, the argument is waived. See Commonwealth v. Dew, 478 Mass. 304, 309 (2017). "We nonetheless review to determine whether there was a substantial risk of a miscarriage of justice." Id. 309-310. For the reasons discussed, there was no abuse of discretion in the judge's conclusion that the information supporting the search warrant was not stale, and established probable cause to search the defendant's laptop and electronic storages devices for evidence of child pornography on the date that the warrant was issued.

Order denying motion to suppress affirmed.

---

determination of probable cause." Commonwealth. v. Upton, 394 Mass. 363, 373 (1985). See Commonwealth v. Alexis, 481 Mass. 91, 98-99 (2018), and cases cited. We have not, however, been called upon to extend additional protections under art. 14, beyond those provided by the Fourth Amendment, to the staleness inquiry in a case involving child pornography, and we discern no reason to address the issue in this case, where the defendant raises it for the first time on appeal.