REPORTED

IN THE COURT OF SPECIAL APPEALS

OF MARYLAND

No. 962

September Term, 2016

JOHN R. FONE

v.

STATE OF MARYLAND

Eyler, Deborah S.,
Arthur,
Wilner, Alan M.
(Senior Judge, Specially Assigned),
JJ.

Opinion by Eyler, Deborah S., J.

Filed: June 6, 2017

A jury in the Circuit Court for Montgomery County convicted John R. Fone, the appellant, of ten counts of distribution of child pornography. The court sentenced him to five years for each count, with the sentences to run concurrently, and suspended the sentences in favor of a five-year term of supervised probation.

The appellant presents four questions for review, which we have condensed and rephrased as three:

> I. Did the circuit court err by denying his motion to suppress from evidence pornographic images of children seized in a search of his laptop computer in his townhouse?
>
> II. Did the trial court err or abuse its discretion by permitting the State's expert witness to opine about certain activity on the appellant's laptop computer immediately before and after pornographic images of children were shared?
>
> III. Was the evidence legally sufficient to support the appellant's convictions?

For the following reasons, we shall affirm the judgments of the circuit court.

FACTS AND PROCEEDINGS

The Child Exploitation Unit ("CEU") operates within the Special Victims Investigations Division ("SVID") of the Montgomery County Police Department ("MCPD"). On January 2, 2015, the CEU received information from the National Center for Missing and Exploited Children ("NCMEC") that an image of child pornography had been attached to an email on a gmail account with the address CaptainJRF@gmail.com, accessed from an Internet Protocol ("IP") address in Germantown. The NCMEC had received that information from Google, which operates gmail.

MCPD Detective Louvenna Pallas, who was working in the CEU, investigated the information and on March 18, 2015, applied for and obtained a search warrant for the appellant's townhouse in Germantown. That same day, she and MCPD Detective Robert Onorio went to the townhouse to execute that search warrant. They knocked on the door and the appellant answered. They asked if they could come inside and speak to him, and he consented.

The detectives sat down with the appellant at his dining room table and talked to him for over an hour. With the appellant's consent, Detective Pallas audio recorded their conversation. The appellant told them he was married with two adult children, neither of whom lived at home. His wife had been diagnosed with Alzheimer's disease six years earlier, and he was her primary caregiver. She was upstairs sleeping during the interview.

Detectives Pallas and Onorio asked the appellant if he had a gmail account; he replied that he did. He identified his email address as "CaptainJRF6969@gmail.com." They asked if he had any other email accounts, such as an account with an address of CaptainJRF@gmail.com. He replied that he "might have had that."[1]

The detectives inquired about the appellant's internet usage. He acknowledged having pornography on his computer but denied having any "inappropriate images of children." He primarily used a Gateway laptop computer ("laptop"), which he kept in the

[1] The appellant later confirmed that he had used that email address. He also identified two other email accounts he used: NudistJohn6969@yahoo.com and CaptJRF6969@verizon.net.

basement of the townhouse. He said he spent a couple of hours each day in online chatrooms and also spent time on Yahoo! Messenger, which is an instant messaging program. He had an account with Flickr, an online photo storage site, under the name "NudistJohn6969."

Detective Onorio asked the appellant whether they could search his laptop and he agreed. Detective Onorio accompanied the appellant to the basement of the townhouse to retrieve the laptop. While the interview continued, Detective Onorio inspected the contents of the laptop. He received permission from the appellant to run a computer program to scan the laptop for child pornography. That program did not work, however, so Detective Onorio carried out a manual search of the laptop. The appellant told the detectives he engaged in "fantasy chats" on the laptop about sexual activity with children. He denied ever having exchanged any child pornography images or videos. He said that on one occasion the previous year a "guy" had sent him two images that he had looked at for "about 10 seconds" and then deleted. One image depicted an infant and the other image depicted "a child in pain."

The appellant said he "d[id] it all" in caring for his wife. His sister had taken care of his wife "once," when he was out of town, but that time he had "left [his wife] at [his] sister's house." His son lived in Seattle. A "good friend" who lived in Phoenix also had taken care of his wife for him.

Detective Onorio located images of what the CEU calls "child erotica" on the laptop. "Child erotica" are images of children in "sexually exploitative positions and dress" that do not meet the definition of child pornography. He asked the appellant if it

was "fair to say [he had] a sexual attraction to children in a fan[tasy] component?" The appellant replied, "Not to children, well yeah." Detective Onorio inquired about the appellant's "age of attraction," noting that his internet searches suggested he was attracted to children from infancy through their teenage years. The appellant replied, "Yeah." He claimed there was no chance that he had child pornography on his laptop, however.

As he continued his manual search of the laptop, Detective Onorio located an image he believed to be child pornography. At that point, he stopped the interview and advised the appellant that the detectives had a search warrant for his house. The detectives seized the laptop and an external hard drive for it that was in the basement where the laptop had been. They also seized a computer tower for a desktop computer that was in the master bedroom. The appellant was not placed under arrest at that time.

Detective Onorio made copies of the hard drives from the devices seized at the appellant's townhouse and provided the copies to the MCPD Electronic Crimes Unit ("ECU"). Detective William Heverly, with the ECU, analyzed the digital copies. From the appellant's laptop, he located ten images of child pornography and numerous internet searches, websites visited, and chat sessions that were associated with child pornography. The ten images had been sent by the appellant to an unknown third party on August 24, 2014.

On September 24, 2015, the appellant was arrested and charged with ten counts of possession of child pornography and ten counts of distribution of child pornography. He later filed a pre-trial motion to suppress the evidence seized from his townhouse.

On April 8, 2016, the court held a suppression hearing. Among other things, the appellant argued that the search warrant was issued based upon information that was stale and therefore did not give rise to probable cause. The court denied the suppression motion, rejecting the staleness argument and ruling, in the alternative, that even if probable cause was lacking the detectives relied upon the warrant in good faith. The appellant filed a motion for reconsideration, which was denied.

Before trial, the State entered a *nolle prosequi* on the possession counts.

A four day jury trial commenced on May 2, 2016. The State called Detective Pallas, Detective Onorio, and Detective Heverly, who was accepted as an expert in digital forensic analysis. The audio recording of the appellant's March 18, 2015 interview with the police was played for the jury, with minor redactions.

Detective Heverly testified that there were two user accounts associated with the appellant's laptop: one under the name "John" and one under the appellant's wife's name. The appellant's wife's account was password protected and had been accessed just 7 times, with the last access in January 2013. The "John" account was not password protected and had been accessed 2,937 times. The ten images of child pornography that formed the basis for the charges had been accessed from the "John" account on the laptop and sent to an unknown third party via Yahoo! Messenger on August 24, 2014, between 3:41 p.m. and 3:47 p.m.

Detective Heverly determined that fifteen minutes before that six-minute Yahoo! Messenger session, a user of the "John" account had accessed the Flickr account the appellant identified as his during the police interview and the

CaptainJRF6969@gmail.com gmail account, which the appellant also had identified as his. Five minutes after the end of the Yahoo! Messenger session, a user of the "John" account had accessed that same gmail account. A user of the "John" account also had accessed a particular chatroom before and after the Yahoo! Messenger session. Detective Heverly further testified that the external hard drive seized from the appellant's townhouse had been plugged into the laptop before and after the Yahoo! Messenger session and images from it had been accessed.

In his case, the appellant presented his own digital forensic analysis expert, Patrick Siewart, who testified that it was possible that a user other than the appellant had uploaded and sent the ten child pornography images. He further testified that laptops are portable, and therefore the images in question could have been sent when the appellant's laptop was outside of Montgomery County or outside of Maryland. He suggested that the MCPD should have subpoenaed the IP address logs for the appellant's internet service provider ("ISP") for August 24, 2014, to determine whether the laptop was connected to the internet at the appellant's townhouse on that date.

The appellant's motion for judgment of acquittal at the close of all the evidence was denied.

After conviction and sentencing, the appellant noted a timely appeal. We shall include additional facts in our discussion of the issues.

DISCUSSION

I.

Denial of the Motion to Suppress

In his pre-trial motion to suppress the evidence the police seized from his townhouse, the appellant argued that the warrant was lacking in probable cause for several reasons, including, as pertinent here, that the affidavit in support of the warrant application "fail[ed] to state the date of the events relied upon to show probable cause . . . [making it impossible] to determine the remoteness in time between the facts observed and the issuance of the warrant, rendering the probable cause stale." In other words, the appellant maintained that because the warrant application did not disclose when the image of child pornography was attached to the CaptainJRF@gmail.com account, that event was not shown to be close enough in time to the date of the warrant application not to be stale.[2]

At the suppression hearing, the warrant application was introduced into evidence by joint stipulation. No testimony or other evidence was introduced.

The warrant application was sworn out by Detective Pallas on March 18, 2015, and the warrant was issued and executed that same day. In the affidavit, Detective Pallas detailed her experience, identified the location to be searched, listed the items to be seized, and averred:

> On 01-02-15, the [NCMEC] cyber tipline received a complaint from Google that an image containing child pornography was attached to the Google email address, captainjrf@gmail.com which may or may not have been sent. (Cybertip #3384307)
>
> The following is a description of the attached image:
>
> 1. Jpeg image titled: 39601_15

[2] It appears that the image of child pornography that Google reported to the NCMEC on January 2, 2015, is not one of the ten images of child pornography the appellant later was charged with possessing and distributing on August 24, 2014.

> This image depicts an adult female performing fellatio on a male toddler's penis.
>
> Your affiant through her training, knowledge, and experience identified the above described image as being child pornography.
>
> Google provided an IP address, date, and time of the suspected uploaded image. A preservation letter was also sent to Google, Inc. to preserve the account information pending warrant service.

Detective Pallas further attested that, using the IP address, she determined that the computer associated with the image was located in Germantown and used a Verizon internet account. She obtained Verizon subscriber information for that account, which was registered to the appellant at an address in Germantown. A Department of Assessments and Taxation search revealed that the address was a townhouse owned by the appellant and his wife. A criminal history background check showed that the appellant had been arrested and charged with public masturbation in Jacksonville, Florida, in 1986.

Detective Pallas further averred in the warrant application that, based on her training and experience, "[s]ubjects who view or collect child pornography value their collections and often go to great lengths to organize and protect their collections including concealing the images on computer media." Moreover, "when subjects possessing child pornography conceal or delete it to avoid detection . . . it is possible to recover files and data from computer media in hidden areas or after it has been deleted."

Before the suppression court, the appellant argued that the information contained within the four corners of the warrant was stale, and therefore the warrant was not

supported by probable cause.[3] The State responded that staleness was not an issue because, unlike drug evidence that is likely to "dissipate" because the drugs will be "used," child pornography stored on a digital device is a "collector's item." Alternatively, the State argued that even if the information in the warrant was stale, the evidence seized should not be excluded because Detectives Pallas and Onorio had relied upon the warrant in good faith.

In rejecting the staleness argument, the suppression court, quoting *United States v. Seiver*, 692 F.3d 774, 777 (7th Cir. 2012), stated that it was persuaded that staleness "'is highly relevant to the legality of a search for a perishable or consumable object like cocaine but rarely relevant when it is a computer file.'" The court emphasized that computer files, even if deleted, can be recovered. The court also found that Detective Pallas's averments in the warrant affidavit, based upon her 14 years of experience as an SVID detective, about "the habits and propensities of those who view or collect child pornography," further supported the view that it is likely that a computer image of child pornography will be saved (or will be recoverable even if deleted).

The court reasoned that given all of the above, the "issue of when did this possession occur . . . doesn't matter much because it is still on the computer until destroyed and that there are ways to get these images back or to recover these images

[3] This was not the appellant's primary argument. His primary argument, which he does not raise on appeal, was that the warrant was not supported by probable cause because the tip from Google was inadmissible hearsay, was uncorroborated, and was unreliable. Defense counsel did not touch on the staleness argument until he was given an opportunity for rebuttal.

even if they have been deleted twice by a person who has access to the computer." Moreover, the court pointed out, federal law requires ISPs, including Google, to report suspected child pornography to the NCMEC "as soon as reasonably possible." *See* 18 U.S.C. § 2258A(a)(1). Thus, it reasonably could "assume that the existence of the picture [was] fairly recent in time," relative to the date of the tip (January 2, 2015).

Alternatively, the court ruled that even if the warrant was lacking in probable cause because it was based on stale information, Detectives Pallas and Onorio acted in good faith in executing it, under *United States v. Leon*, 468 U.S. 897 (1984). The court opined that there was "nothing so glaring about this search warrant that would suggest to a well-trained officer that he [or she] could not rely on that warrant particularly since it [was] linked to [the appellant]'s address and computer very well." Moreover, the "description of the contraband [was] clear and d[idn't] leave anything subject to interpretation" and the source of the tip was Google, which did "have some degree of reliability."

The appellant filed a motion for reconsideration addressing only the issue of staleness, which the State opposed.[4] On the first day of trial, the court heard argument on that motion and denied it.

Before this Court, the appellant contends the suppression court erred by "ruling that the evidence contained within the search warrant affidavit was not stale." He relies upon numerous federal cases on staleness of probable cause that hold that information

[4] The appellant's motion does not appear in the record, but the State's opposition to it does.

leading police to believe that child pornography is present on a computer *can* become stale over time; that each case must be considered on its unique facts; and that a period of more than a year is often too remote. The appellant argues that because the warrant affidavit established only that one image of suspected child pornography was attached to an email on an unknown date before January 2, 2015, and there were no facts showing that Detective Pallas took any additional investigative steps to determine when that image was uploaded, the court could not assess whether the length of time was too remote. He maintains, moreover, that Detectives Pallas and Onorio could not "claim objective good faith when they relied upon a search warrant that was so lacking in probable cause."

The State responds that the warrant application in this case was not the type of conclusory, bare-bones application that falls outside the broad protections of *Leon*, and the suppression court correctly ruled that the detectives relied upon the warrant in good faith. The State maintains that because the good faith ruling was correct, this Court need not address the staleness issue; and if we do, the issuing judge had a substantial basis to believe that probable cause supporting the warrant was not stale, and therefore child pornography would be found at the appellant's townhouse.

We shall address staleness and good faith.

-a-

Our standard of review when considering a facial challenge to a search warrant is well-established:

> We determine first whether the issuing judge had a substantial basis to conclude that the warrant was supported by probable cause. *State v. Amerman*, 84 Md. App. 461, 463–64, 581 A.2d 19, 20 (1990). We do so not

> by applying a *de novo* standard of review, but rather a deferential one. The task of the issuing judge is to reach a practical and common-sense decision, given all of the circumstances set forth in the affidavit, as to whether there exists a fair probability that contraband or evidence of a crime will be found in a particular search. *Illinois v. Gates*, 462 U.S. 213, 238–39, 103 S.Ct. 2317, 2332, 76 L.Ed.2d 527, 548 (1983). The duty of a reviewing court is to ensure that the issuing judge had a "substantial basis for . . . conclud[ing] that probable cause existed." *Id*. (Quotation and citations omitted); *Birchead v. State*, 317 Md. 691, 701, 566 A.2d 488, 492–93 (1989); *Potts v. State*, 300 Md. 567, 572, 479 A.2d 1335, 1338 (1984) (Quotation and citation omitted). The U.S. Supreme Court explained in *Gates* that the purpose of this standard of review is to encourage the police to submit to the warrant process. *Gates,* 462 U.S. at 237 n.10, 103 S.Ct. at 2331 n.10, 76 L.Ed.2d at 547 n.10.

Greenstreet v. State, 392 Md. 652, 667–68 (2006).

"One of the factors in the 'probable cause puzzle' concerns the staleness of the information contained in an affidavit supporting a search warrant application." *Behrel v. State*, 151 Md. App. 64, 88 (2003) (quoting *West v. State*, 137 Md. App. 314, 327–28 (2001)). "There is no 'bright-line' rule for determining the 'staleness' of probable cause; rather, it depends upon the circumstances of each case, as related in the affidavit for the warrant." *Connelly v. State*, 322 Md. 719, 733 (1991). In making that assessment, the court considers whether "the 'event[s] or circumstance[s] constituting probable cause, occurred at . . . [a] time . . . so remote from the date of the affidavit as to render it improbable that the alleged violation of law authorizing the search was extant at the time[.]'" *Patterson v. State*, 401 Md. 76, 92 (2007) (quoting *Peterson v. State*, 281 Md. 304, 314 (1977)). That assessment turns on the particular facts of the case:

> The ultimate criterion in determining the degree of evaporation of probable cause, however, is not case law but reason. The likelihood that the evidence sought is still in place is a function not simply of watch and calendar but of variables that do not punch a clock: the character of the crime (chance

> encounter in the night or regenerating conspiracy?), of the criminal (nomadic or entrenched?), *of the thing to be seized (perishable and easily transferable or of enduring utility to its holder?)*, of the place to be searched (mere criminal forum of convenience or secure operational base?), etc. The observation of a half smoked marijuana cigarette in an ashtray at a cocktail party may well be stale the day after the cleaning lady has been in; the observation of the burial of a corpse in a cellar may well not be stale three decades later. The hare and the tortoise do not disappear at the same rate of speed.

Andresen v. State, 24 Md. App. 128, 172 (1975) (emphasis added).

Several federal courts addressing staleness of probable cause in the context of child pornography stored on digital devices have reasoned that because digital images have a "potentially infinite lifespan," *United States v. Elbe*, 774 F.3d 885, 891 (6th Cir. 2014), *cert. denied*, 135 S.Ct. 1573 (2015), "'the passage of time alone' cannot demonstrate staleness." *United States v. Burkhart*, 602 F.3d 1202, 1206 (10th Cir. 2010) (quoting *United States v. Mathis*, 357 F.3d 1200, 1207 (10th Cir. 2004)). In *Seiver*, 692 F. 3d at 775–76, for example, the Seventh Circuit held that a seven-month delay from the date that child pornography images were downloaded from the internet to the defendant's computer to the date a search warrant for the defendant's computer was applied for did not render the information stale. The court opined:

> "Staleness" is highly relevant to the legality of a search for a perishable or consumable object, like cocaine, but rarely relevant when it is a computer file. Computers and computer equipment are "not the type of evidence that rapidly dissipates or degrades." *United States v. Vosburgh*, 602 F.3d 512, 529 (3d Cir. 2010). Because of overwriting, it is *possible* that the deleted file will no longer be recoverable from the computer's hard drive. And it is also *possible* that the computer will have been sold or physically destroyed. And the longer the interval between the uploading of the material sought as evidence and the search of the computer, the greater these possibilities. But rarely will they be so probable as to destroy probable cause to believe that a search of the computer will turn up the evidence sought; for probable cause

> is far short of certainty—it "requires only a probability or substantial chance of criminal activity, not an actual showing of such activity," *Illinois v. Gates*, 462 U.S. 213, 244 n. 13, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983), and not a probability that exceeds 50 percent ("more likely than not"), either. *Hanson v. Dane County*, 608 F.3d 335, 338 (7th Cir. 2010).

Id. at 777 (emphasis in original).

> The *Seiver* court recognized that
>
> after a *very* long time, the likelihood that the defendant still has [a particular] computer, and if he does that the file hasn't been overwritten, or if he's sold it that the current owner can be identified, drops to a level at which probable cause to search the suspect's home for the computer can no longer be established.

Id. (emphasis in original). Seven months was far too short a period of time for that to occur, however. *See also United States v. Carroll*, 750 F.3d 700, 704-05 (7th Cir. 2014) (five-year gap between date victim alleged she was molested by defendant, at which time he showed her images of child pornography and took digital images of her genitals, and date of warrant application was not so remote as to render probable cause to search the defendant's home and seize cameras and other digital devices stale); *Burkhart*, 602 F.3d at 1206-07 (information pertaining to an email between child pornography distributor and the defendant two years and four months before issuance of a search warrant not stale); *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008) (lapse of three years between the defendant's purchase of digital child pornography images and warrant application did not render search warrant stale); *but see United States v. Greathouse*, 297 F.Supp. 2d 1264, 1272-73 (D. Ore. 2003) (information that child pornography was distributed from a computer f: drive 13 months before a search warrant was applied for was stale, so search warrant was not supported by probable cause).

In the case at bar, the March 18, 2015 warrant application showed that Google made its disclosure to the NCMEC about ten weeks earlier, on January 2, 2015. NCMEC then reported the information from Google to the MCPD, which engaged in the investigation set forth in the affidavit. Google gave the information to NCMEC pursuant to a federal statute mandating ISPs to notify the NCMEC of suspected child pornography "as soon as reasonably possible." We agree with the suppression court that, given that statutory mandate, the judge to whom the warrant application was presented rationally could infer that the image of suspected child pornography was attached to an email on a day reasonably close in time to January 2, 2015, and certainly within a few years. In this case, in which the lapse between the report from Google and the issuance of the search warrant was only three months and the lapse between the emails of August 24 and the warrant was only seven months, Detective Pallas's averments about the habits of possessors of child pornography and the ability of the police "to recover files and data from computer media [even] after it has been deleted" gave rise to a substantial basis for the issuing judge's probable cause determination. *See Behrel*, 151 Md. App. at 90 ("In analyzing the issue of staleness, 'the expertise and experience of the officer are to be taken into account in applying the Fourth Amendment probable cause test,' even if 'the officer would not qualify as an expert witness on the subject.'" (quoting 2 LaFave, § 3.2(c), at 38–39, 38 n.70)).

-b-

If we agreed with the appellant that the information in the warrant application was stale, which we do not, we nevertheless would agree with the suppression court that the good faith exception applied.

Evidence seized without a warrant *or* based upon a warrant not supported by probable cause may be subject to exclusion. *See, e.g., Agurs v. State*, 415 Md. 62, 76 (2010). Unlike a warrantless search, however, "searches pursuant to a warrant will rarely require any deep inquiry into reasonableness, for a warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *Leon*, 468 U.S. at 922 (citations omitted). Thus, "[i]n the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit *or could not have harbored an objectively reasonable belief in the existence of probable cause*." *Id*. at 926 (emphasis added).

The *Leon* Court outlined four scenarios in which the good faith exception will not apply:

> (1) the magistrate was misled by information in an affidavit that the officer knew was false or would have known was false except for the officer's reckless regard for the truth;
> (2) the magistrate wholly abandoned his detached and neutral judicial role;
> (3) the warrant was based on an affidavit that was so lacking in probable cause as to render official belief in its existence entirely unreasonable; and
> (4) the warrant was so facially deficient, by failing to particularize the place to be searched or the things to be seized, that the executing officers cannot reasonabl[y] presume it to be valid.

Id. at 923. The appellant relies only upon the third scenario.

Where, as here, the facts are not in dispute, we review the suppression court's ruling on "the applicability of the *Leon* good faith exception to the exclusionary rule . . . *de novo*[.]" *Patterson*, 401 Md. at 104–05. In assessing whether the warrant application was "so lacking in probable cause as to render official belief in its existence entirely unreasonable," *Leon*, 468 U.S. at 923, we apply an objective test to determine whether "officers, exercising professional judgment, could have reasonably believed that the averments of their affidavit related a present and continuing violation of law, not remote from the date of their affidavit, and that the evidence sought would be likely found at [the place identified in the affidavit]." *Connelly*, 322 Md. at 735. As this Court has explained, that reasonable belief test will not be satisfied when the warrant application contains "nothing beyond mere conclusions." *State v. Jenkins*, 178 Md. App. 156, 203 (2008).

In the case at bar, the warrant application was not conclusory or bare bones. It gave the date and the substance of the Google tip to the NCMEC; the nature of the pornographic image uploaded; the investigation into the IP address associated with the upload; the means to establish that the appellant lived at that address; the types of devices that might be used to store child pornography; expert information about the habits of collectors of child pornography; and expert information about forensic techniques to recover deleted computer files. Although the date the image was attached to the email was not included, the date Google informed the NCMEC about the image, which was just over three months before the warrant application, supported a reasonable belief that someone at the appellant's townhouse had engaged in a violation of the law (possession

of child pornography) within months of the warrant application and, in light of the other averments, that evidence of that possession could be found on a device located at that address, even if it had since been deleted.

II.

State's Expert's Testimony

As circumstantial proof of the appellant's criminal agency, the State presented evidence, through Detective Heverly, that 1) the appellant's gmail account and his Flickr account were accessed from his laptop within 15 minutes before the six minute Yahoo! Messenger session in which the ten images of child pornography were distributed by means of that laptop; 2) his gmail account also was accessed from that laptop within five minutes after that session; 3) pornographic images of adult males were accessed by the appellant's laptop from his external hard drive soon before and after the critical Yahoo! Messenger session; and 4) the "Silver Daddy" chatroom was accessed from the appellant's laptop soon before and after the Yahoo! Messenger session. The last two categories of evidence were relevant because the appellant told the police in his interview that he was bisexual, had had two long-term sexual relations with men over the past several decades, and viewed adult gay pornography and participated in gay sexual chatrooms such as "Silver Daddy."

The appellant contends the State violated Rule 4-263(d), governing mandatory discovery disclosures by the State in a criminal case, by not disclosing the specific information about the gmail and Flickr account access, and consequently the court erred

by not excluding Detective Heverly's testimony in that regard. (The appellant does not raise any issue about the evidence on the external hard drive.)

The State responds that this issue is not preserved for review and, in any event, the court did not err or abuse its discretion by permitting Detective Heverly to testify about the account activity on the laptop soon before and after the incriminating Yahoo! Messenger session.

On March 30, 2016, the State sent a letter to defense counsel stating that it intended to call Detective Heverly as an expert witness in "digital forensic examination"; that he would testify that his examination of the laptop revealed that the "contraband charged in counts 1-10 was distributed via Yahoo! Messenger on August 24, 2014"; and that he would "further testify that his examination revealed that both prior-to and after the distribution of the contraband charged in counts 1-10, the user [of the laptop] accessed images files and video files of pornography, specifically pornography depicting adult men engaged in various sexual activities with each other."

Before trial, the State provided the defense a summary of the Internet Evidence Finding report ("IEF") that Detective Heverly prepared after he examined the copies of the hard drives for the appellant's laptop and other devices. The State could not provide the full IEF report to the defense because it contained prohibited images that could not be shared. The full IEF report included the information about the gmail and Flickr accounts used immediately before and after the Yahoo! Messenger session. The State made open file discovery available, so the defense had access to the full IEF report. And, as part of open file discovery, the State made the copies of the hard drives that were searched by

Detective Heverly and were the subject of his IEF report available for inspection by the defense expert. Indeed, the defense expert inspected them, twice, performing his own forensic examination and preparing his own IEF report.

At the outset of the proceedings on May 5, 2016, which was the third day of trial and the day Detective Heverly was expected to testify, the prosecutor advised the court that he planned to use a demonstrative exhibit titled "Timeline analysis for August 24, 2014" ("Exhibit 11") that showed laptop user access of the Flickr account and the gmail account in the periods shortly before and after the Yahoo! Messenger session. The prosecutor explained that Detective Heverly's testimony about user access before and after the Yahoo! Messenger session would be "circumstantial evidence of who was using the laptop at the time of the distribution [of child pornography]." The prosecutor maintained that the information in Exhibit 11 had been disclosed to defense counsel in the March 30, 2016 expert disclosure.

Defense counsel responded that the prosecutor had not disclosed that the State intended to present evidence that a user of the laptop accessed the Flickr account or the gmail account, only that a user of the laptop had viewed pornography involving adult gay men. The prosecutor disagreed, taking the position that the expert disclosure was sufficient and, in any event, because the defense expert had been given full access to the copy of the hard drive for the laptop, the defense could not claim unfair surprise about any information on the laptop.

The court denied the motion *in limine*, ruling that Detective Heverly could testify about the user access as shown on Exhibit 11. Defense counsel "note[d] [his] objection

to the expert testifying as to the usage of the computer shortly prior to and subsequent thereto because that was not something that was provided [in discovery]." He did not seek a continuing objection.

Detective Heverly was called as the second witness that day. He was accepted as an expert in digital forensic analysis by stipulation. After he testified generally about his analysis of the laptop hard drive, the Yahoo! Messenger program, and the ten images of child pornography sent via Yahoo! Messenger over six minutes on August 24, 2014, the prosecutor approached the stand and showed him Exhibit 11 to refresh his recollection about the start time (3:41 p.m.) and end time (3:47 p.m.) of that Yahoo! Messenger session. Defense counsel did not object to any of this line of inquiry.

Later in Detective Heverly's direct examination, the prosecutor asked: "And how do you go about trying to identify the person who is sitting at the computer? The user." Detective Heverly responded that he tries to "find data and artifacts that will kind of help us determine who that person was." He gave as an example a user who works on his resume, then engages in "illegal activity," and then goes back to working on his resume. He explained, "So we[] look for activity before and after." He was asked if he had "attempt[ed] to ascertain anything that was going on on [the laptop] that the user was accessing at the time, 3:41 [p.m.] to 3:47 [p.m.] on August 24th of 2014?" He responded that he had "specifically searched for activity right around that date to see what was going on." He did not find any other user activity *during* the Yahoo! Messenger session, but he did find user activity just before and after that session. He then testified about the gmail and Flickr accounts access as reflected on Exhibit 11. These questions all were

asked, and Detective Heverly's answers all were given, without any objection or motion to strike.

When Detective Heverly was asked whether he was able to determine that a user had accessed the external hard drive seized from the appellant's basement around the time of the Yahoo! Messenger session, defense counsel objected and a bench conference was held. The prosecutor explained that Detective Heverly was going to testify that images were accessed from an external hard drive plugged into the laptop immediately before and again immediately after the 6 minute Yahoo! Messenger session. Defense counsel argued that the March 30, 2016 expert disclosure letter did not reveal that the State's expert would testify that the external hard drive had been accessed at those times. The court disagreed and overruled the objection.

The prosecutor then resumed questioning Detective Heverly about the access of the external hard drive. The questioning spans more than two pages of the transcript. Defense counsel did not lodge any further objections.

The prosecutor subsequently sought to introduce Exhibit 11 into evidence. The court denied that request, ruling that it was a demonstrative exhibit that had not been disclosed to defense counsel in a timely manner.

We agree with the State that the issue the appellant raises on appeal—whether the trial court erred by allowing Detective Heverly to testify about the laptop user accessing his gmail and Flickr accounts close in time to the Yahoo! Messenger session in which the child pornography images were distributed—is not preserved for review. "It is well-established that a party opposing the admission of evidence 'shall object' at the time the

evidence is offered or as soon thereafter as the grounds for objection become apparent. *Wimbish v. State* 201 Md. App. 239, 260–61 (2011) (quoting Md. Rule 4-323(a)) (additional citations omitted). If not, the objection is waived and the issue is not preserved for review. *Id.* at 261. Also, "to preserve an objection, a party must either 'object each time a question concerning the [matter is] posed or . . . request a continuing objection to the entire line of questioning.'" *Id.* (quoting *Brown v. State*, 90 Md. App. 220, 225 (1992)). "Th[is] requirement of a contemporaneous objection at trial applies even when the party contesting the evidence has made his or her objection known in a motion in limine[.]" *Id.*

Here, the appellant did not object to any of the long line of questions that elicited the evidence he complains about on appeal. His only objection was to the admission of Detective Heverly's testimony about the images of pornography on the external hard drive, which is not the evidence being challenged on appeal. Moreover, we disagree with the appellant's argument in his reply belief that there was sufficient temporal proximity between the trial court's denial of the motion *in limine* and the direct examination of Detective Heverly that the failure to make a contemporaneous objection should be excused. Detective Heverly's testimony was preceded by the cross-examination and redirect examination of Detective Onorio. *See, e.g., Hickman v. State*, 76 Md. App. 111, 117-18 (1988) ("temporal closeness" exception to the contemporaneous objection rule applies only when the court rules (or reiterates a prior ruling) immediately prior to the objectionable testimony being elicited or evidence being offered). Also, at the close of

the motion *in limine*, the appellant could have requested a continuing objection but did not.

In any event, we would not find merit in this issue even if it were preserved for review. Rule 4-263(d) governs mandatory discovery disclosures by the State. At subsection (d)(8), "Reports or Statements of Experts," it requires the State to disclose, in pertinent part, "[a]s to each expert consulted by the State's Attorney . . . the expert's name and address, the subject matter of the consultation, the substance of the expert's findings and opinions, and a summary of the grounds for each opinion." Also, the State is required to provide the defense "the opportunity to inspect and copy all written reports or statements made in connection with the action by the expert, including the results of any physical or mental examination, scientific test, experiment, or comparison." *Id.*

The March 30, 2016 disclosure by the State was non-specific, but referred to video images and files accessed by the laptop user before and after the Yahoo! Messenger session in which the images of child pornography were distributed. The details were contained in the full IEF report prepared by Detective Heverly.

As noted, the State could not give that report to the defense as it contained prohibited images, so the State gave the defense a summary and the opportunity for the defense to have its own expert review the full IEF report in person. The dispute during the motion *in limine* argument was over whether the State in fact did so. Defense counsel asserted that the State did not; the prosecutor asserted that the State did. The court found that the State had provided the report, and we cannot say that that finding was clearly erroneous. Moreover, there was no dispute that the defense expert in fact examined the

hard drive copy for the laptop more than once and that the State offered to have Detective Heverly review it with him. On this record, the court did not err or abuse its discretion in denying the motion *in limine*.

III.

Sufficiency of the Evidence

Finally, the appellant contends the evidence was legally insufficient to sustain his convictions for distribution of child pornography for two reasons. First, the State failed to establish that he was the person using the laptop when the 10 images were sent via the Yahoo! Messenger program. Second, the State failed to prove territorial jurisdiction, *i.e.*, that the criminal conduct occurred in Maryland.

The State responds that it presented ample circumstantial evidence from which jurors reasonably could infer that the appellant was the user of the laptop when the images of child pornography were accessed and transmitted and that he was at his home in Maryland at the time of the charged conduct. We agree with the State.

As this Court has explained:

> "The standard for appellate review of evidentiary sufficiency is whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *State v. Smith*, 374 Md. 527, 533, 823 A.2d 664 (2003) (citations omitted). "Weighing the credibility of witnesses and resolving any conflicts in the evidence are tasks proper for the fact finder." *State v. Stanley*, 351 Md. 733, 750, 720 A.2d 323 (1998). In addition, we give "'due regard to the [fact finder's] finding of facts, its resolution of conflicting evidence, and, significantly, its opportunity to observe and assess the credibility of witnesses.'" *Moye v. State*, 369 Md. 2, 12, 796 A.2d 821 (2002) (quoting *McDonald v. State*, 347 Md. 452, 474, 701 A.2d 675 (1997) (quoting *State v. Albrecht*, 336 Md. 475, 478, 649 A.2d 336 (1994))).

Larocca v. State, 164 Md. App. 460, 471-72 (2005) (*en banc*).

The appellant relies upon several federal cases holding that evidence was legally insufficient to prove criminal agency vis-à-vis charges of possession of child pornography when someone other than the defendant had access to the digital device and was not excluded as the user. *See United States v. Lowe*, 795 F.3d 519, 523-24 (6th Cir. 2015) (evidence insufficient to prove criminal agency when the defendant, his wife, and his "adoptive son" had access to the laptop and were not excluded as possible users); *United States v. Moreland*, 665 F.3d 137, 151-52 (5th Cir. 2011) (evidence insufficient to prove criminal agency when child pornography was found on a computer in the home shared by the defendant, his wife, and his father, and there was evidence that the defendant's father frequently used the computer late at night while the defendant and his wife slept).

In the case at bar, in contrast, the evidence viewed in the light most favorable to the State did not reveal any actual or even potential alternative users. The appellant lived in a townhouse with his wife, who was suffering from Alzheimer's disease. The appellant's wife had been diagnosed around 2009, more than four years before the Yahoo! Messenger session. The appellant admitted to the police that the laptop in his basement belonged to him and that he spent several hours every day using it there. In his police interview, the appellant did not claim that anyone else had used his laptop or even that anyone else frequented his townhouse, either to visit or help care for his wife. He openly informed the police about his bisexuality and that his current partner, of eight

years, lived in Atlanta and never came to his house to visit.[5] He acknowledged having several gmail accounts (and provided the addresses); having a Flickr account (and provided his user name); visiting the Silver Daddy chatroom (and provided his user name); and using Yahoo! Messenger.

The appellant further admitted that he was sexually attracted to children; that he engaged in fantasy chats about sexual activity with children; and that he frequently viewed pornography, including images of adult men engaging in sex acts, on his laptop.

The evidence pertinent to April 24, 2014, the date of the distribution, showed that a user of the appellant's laptop accessed a gmail account belonging to the appellant and a Flickr account belonging to the appellant about 15 minutes before the 10 images were sent via Yahoo! Messenger. Within two minutes of the end of that session, a user of the appellant's laptop again accessed those same two accounts. A user of the appellant's laptop also accessed an external hard drive kept in the appellant's basement before and after the Yahoo! Messenger session, accessing images depicting adult males engaged in sexual acts. This plainly was evidence from which reasonable jurors could infer that the appellant was the person using the laptop before, during, and after the Yahoo! Messenger session.

The evidence also was legally sufficient to prove that the criminal conduct took place in Maryland. Detective Heverly testified that he had detected "artifacts" on the laptop showing that it had been connected to the internet in the appellant's townhouse ten

[5] The appellant's family members knew he was bisexual and knew his partner, but he had promised his wife he would not bring his partner to their home.

days before the subject images were distributed. As noted, the appellant told police that he used his laptop in his basement and that he had had to "give up all" his activities after his wife became ill, sometime around 2009. There also was evidence that the laptop was connected to an external hard drive on August 24, 2014, both before and after the Yahoo! Messenger session. This was evidence from which a reasonable juror could infer that the laptop was located in the appellant's home in Maryland, where he stored his laptop and the external hard drive, at the time of the Yahoo! Messenger session.

JUDGMENTS AFFIRMED. COSTS TO BE PAID BY THE APPELLANT.