United States Court of Appeals
For the First Circuit

No. 17-1696

UNITED STATES OF AMERICA,

Appellee,

v.

DAVID MOREL, JR.,

Defendant, Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

[Hon. Joseph Laplante, U.S. District Judge]

Before

Lynch, Lipez, and Barron,
Circuit Judges.

Daniel N. Marx, with whom Fick & Marx LLP was on brief, for appellant.

Seth R. Aframe, Assistant U.S. Attorney, with whom Scott W. Murray, United States Attorney, was on brief, for appellee.

April 19, 2019

LYNCH, **Circuit Judge**. After the district court denied his motions to suppress evidence, David Morel, Jr., entered a conditional plea to one count of possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). He was sentenced to seventy months' imprisonment. Morel uploaded child pornography images to a digital album on Imgur, an image hosting website. Law enforcement learned of the images on Imgur from the National Center for Missing and Exploited Children (NCMEC), which had received a report about the images from an anonymous tipster.

On appeal, Morel challenges the district court's determinations that Morel had no reasonable expectation of privacy in the images he uploaded to Imgur or in his internet protocol (IP) address, and that the state warrant to search Morel's computer was supported by probable cause. We affirm.

I.

A. Facts

We describe the findings of fact made by the district court after evidentiary hearings on the motions to suppress. We supplement those facts, as necessary, with other facts from the record.

1. CyberTipline Report

The investigation of Morel began with an anonymous report submitted to NCMEC. NCMEC is a non-profit organization that maintains the "CyberTipline," a website through which members

of the public, law enforcement, and others report child exploitation and child pornography. Those using the CyberTipline to make a report are required to include the date, time, and substance of the incident in the report, and may submit reports anonymously. Electronic service providers that "obtain[] actual knowledge of any facts and circumstances . . . from which there is an apparent violation" or a "planned or imminent" violation of statutes concerning child pornography are legally obligated to report such information to NCMEC. 18 U.S.C. § 2258A(a). NCMEC must forward reports it receives to an appropriate law enforcement agency. Id. § 2258A(c).

On November 23, 2013, an unidentified individual submitted a report, which included a list of Uniform Resource Locators (URLs) said to depict child pornography, to the CyberTipline. The list of URLs spanned two pages. This tipster did not include any personal identifying information in the report.[1] NCMEC staff analysts investigated the contents of the report. One of the URLs listed in the report led to a "gallery" or "album" of images hosted by Imgur. Each image in the album also had its own specific URL; an analyst obtained the URLs of the images in the album that appeared to contain child pornography

[1] NCMEC captured the IP address from which the report was sent, but did not take the step of identifying the person(s) associated with that IP address.

without clicking on the individual URLs,[2] and copied those URLs into a report.

On November 26, 2013, NCMEC sent a notice to Imgur summarizing the instances of child pornography reported to have been found on its website, which included URLs of images reported by the tipster. NCMEC's notice asked Imgur to "[p]lease review the reported URL[s] to determine if [they] contain[] content that violates federal and/or state law or your Terms of Service or Member Services Agreement."

After reviewing the reported URLs, Imgur filed reports with NCMEC concerning three images obtained through the CyberTipline, stating that the corresponding URLs flagged by NCMEC appeared to contain child pornography. Imgur attached copies of the three images to the reports. Imgur provided the IP address from which the images were uploaded to Imgur's servers, which was the same for all three images. Imgur also reported that the images were uploaded in November 2013. Imgur then deleted the images from its server. Using a publicly available website, NCMEC looked up the IP address included in Imgur's report and learned that it was associated with a Comcast subscriber in Derry, New Hampshire.

[2] At a suppression hearing, the witness from NCMEC explained, "[t]his staff member did not click on any links . . . . [W]hat they did is they took their mouse, hovered over the images that appeared to depict child pornography, they copied that image location and put it into the report."

On December 6, 2013, Imgur submitted three additional reports of alleged child pornography associated with the same IP address to NCMEC through the CyberTipline. Those images had also been uploaded to Imgur in November 2013. That made a total of six reported images of alleged child pornography from this IP address.

2. The Investigation

NCMEC provided the six reports to the New Hampshire Internet Crimes Against Children Task Force on December 12, 2013, which forwarded the reports to the Derry, New Hampshire Police Department on January 10, 2014. Detective Kennedy Richard, experienced in investigating child pornography and child sexual exploitation, reviewed the images in the reports. He entered the IP address from the reports into a publicly-available website and learned that the IP address was associated with a Comcast account. He then obtained a subpoena requesting information from Comcast about the owner of the IP address. On February 14, 2014, Detective Richard learned that the IP address belonged to a David Morel at Pingree Hill Road in Derry, New Hampshire.

About two weeks earlier, on February 1, 2014, David Morel, Jr., had reported to the Derry Police Department that his laptop computer was stolen during a burglary of the Pingree Hill Road residence. The Derry Police Department recovered the stolen computer and other stolen property the following week. Morel went to the police station on February 7, 2014, and identified the

computer he had reported stolen. The police retained the computer as evidence of the burglary.

In late March 2014, Detective Richard called the Pingree Hill Road residence. Two weeks later, Morel's father called Detective Richard back and stated that his son, David Morel, Jr., had lived at the Pingree Hill Road residence on the date that the images were uploaded in November 2013, but had moved out later, in February 2014. Morel's father stated that he did not use the email address associated with the Comcast account connected to the IP address in question, but that he believed his son used that email address.

On April 16, 2014, Detective Richard sought and obtained a warrant from a New Hampshire state court to search Morel's computer, which was still in police custody. In the affidavit supporting the warrant application, Detective Richard did not attach the six suspected child pornography images, which depicted different girls. The affidavit stated that Detective Richard had worked as a Derry police officer since 1993, and had been a detective for the Derry Police Department since 1999. As a detective, his primary assignment was in the Juvenile Division as an investigator. He had received specialized training concerning sexual assault investigations, including in child abuse and exploitation cases. He had also been a member of the Internet Crimes Against Children Task Force since 2005, and had assisted in

the execution of about fifty search warrants related to possession and distribution of illegal child sexual abuse and exploitation images.

The affidavit described the NCMEC reports and the IP address information connected to Morel. The affidavit also described the nudity and the sexual or sexually suggestive positioning of the girls depicted in each of the six suspected child pornography images. Some images contained more than one girl. The ages of the different girls were described as follows: (1) "A naked female . . . . She appears to be under the age of 10"; (2) "Two naked females . . . both believed to be under the age of 10"; (3) "A female believed to be under the age of 10"; (4) "Two naked females believed to be under the age of 13"; (5) "A naked female [sic] to be under the age of 13"; and (6) "A naked female believed to be under the age of 13." The affidavit specified that some of the other females in the images were of "unknown age." The affidavit did not describe the girls in such terms as "pubescent" or "prepubescent."

Pursuant to the warrant, Detective Richard obtained a forensic copy of the hard drive of Morel's computer, which was still in police custody. He reviewed the contents and saw what he estimated to be about 200 videos and images of child pornography.

On April 28, 2014, Morel was arrested on the charge of attempted possession of child sexual abuse images.[3] Morel was taken into custody and Detective Richard interviewed him at the Derry police station. Morel was given Miranda warnings, waived his Fifth Amendment rights, and admitted to possessing child pornography on his computer.

3. Imgur Terms of Service and Image Hosting Practices

The Imgur Terms of Service stated at the time, in relevant part:

> You can upload images anonymously and share them online with only the people you choose to share them with. If you make them publicly available, they may be featured in the gallery. This means that if you upload an image to share with your friend, only your friend will be able to access it online. However, if you share an image with Facebook, Twitter, Digg, Reddit, et cetera, then it may end up in the gallery.

The following witnesses testified at the suppression hearings: Brianna Walker, an Imgur employee who was an online

[3] At a suppression hearing, Detective Richard testified that he found out later that the reason a Derry prosecutor originally charged Morel with attempted possession of such images is that "[w]ith attempted possession you don't have to prove that it was an actual child depicted in the photo or identify the child." Detective Richard had thought Morel was arrested for possession of child pornography based on the search of his computer, but the prosecutor later told him that "it had to be attempted possession of child pornography" because "[t]hey don't charge possession. They charge attempted possession."

"store manager" and who also handled "user support" and "rules";[4] John Shehan, the vice president of NCMEC; and Detective Richard.

Walker explained that Imgur permits "anonymous uploads," meaning that there is no requirement that a person set up an account to upload images to Imgur. A user can upload photos to Imgur that "everyone in the world can see," and that are available on Imgur's "public gallery." Walker explained that, alternatively, an Imgur user can "make a private album which can only be accessed from your account; however, each image can still be seen by anyone using the direct image link." When asked if an image on a "private" album can "be found in any other particular method," Walker explained, "Google would have crawled through the images so they'd be available . . . if you searched for them." When asked, "is there any way that a person using [Imgur] to upload photos can be sure that their image is private and can never be seen," Walker responded, "No, that's impossible." Walker explained:

> [Y]ou can share the URL [to a private album] with anyone and only those people will be able to see it, but anyone can still access the image by using the URL. So they could guess it, it would still be searchable on Google. So it's impossible for any of this to be completely private . . . . It couldn't be

[4] Walker explained that her role involved not only handling online sales, but also responding to emails from users with complaints or issues, and deleting child pornography and copyrighted images from Imgur.

> found on [Imgur], but . . . you could still guess it or find it on a search engine.

Imgur staff can also view images that users have uploaded to private Imgur albums.

The record does not establish whether Morel chose a private album for the images at issue. Walker first testified that "[i]t's more likely that he selected private, but . . . there's no way to know." She then clarified, "I can circle back and look at his account, but I'm pretty sure it was private." The prosecutor later stated that her "understanding was that the records in regard to this account were no longer kept by [Imgur]."

Walker testified that there was no way for Imgur to track whether Morel shared the URLs of the images he uploaded with anyone, and no way to track whether other people accessed those URLs. Imgur keeps a count of the number of times an image is viewed but does not track whether each viewer is the person who uploaded the image or is a third party.

The IP address of the person who uploads an image to Imgur is accessible only to Imgur staff. Imgur does not actively search or use software to detect child pornography uploaded by users, but when it receives reports of such images, it reviews the images, and if they appear to contain child pornography, Imgur reports them to NCMEC. Imgur then deletes the offending images.

Notice of this policy is included in the Terms of Service, which Imgur users must agree to before using Imgur.

B. Procedural History of Suppression Motions

Morel's first suppression motion sought to suppress images of child pornography obtained from his computer and statements he made during custodial interrogation, arguing that this evidence was obtained pursuant to a warrantless search by Imgur, acting at the instigation of NCMEC. His second motion sought to suppress images obtained from his computer, arguing the computer was searched pursuant to a warrant that lacked probable cause.[5] This second motion also stated that Imgur improperly provided NCMEC with the IP address from which Morel uploaded the images to Imgur.[6]

The district court held evidentiary hearings on the suppression motions on February 24, 2016 (during which the Imgur employee and the NCMEC vice president testified), and September 22, 2016 (during which Detective Richard testified). The district court denied the motions in electronic orders, supplemented by a later written decision. Morel pleaded guilty to one count of

[5] Morel's third motion to suppress (not at issue on appeal) sought to suppress evidence from what he argued was an unconstitutional warrantless arrest.

[6] Morel's second suppression motion did not sufficiently develop this argument concerning Morel's IP address, but defense counsel made the argument at a suppression hearing, and the district court considered it.

possession of child pornography on December 19, 2016, pursuant to a plea agreement, reserving his right to appeal the denial of his first two suppression motions.

On April 14, 2017, the district court entered a written order stating its reasons for denying Morel's suppression motions. United States v. Morel, No. 14-CR-148-JL, 2017 WL 1376363 (D.N.H. Apr. 14, 2017), reconsideration denied, 2017 WL 2773538 (D.N.H. June 26, 2017). The district court determined that Morel had not met his burden of showing that he had a reasonable expectation of privacy in the images uploaded to Imgur because the images were "publicly available" and "[n]o evidence suggests that Morel took affirmative steps to protect the images." Id. at *6. The court also noted that both the anonymous tipster and an NCMEC employee were able to access the images. Id. The court explained that "the uploaded images are more akin to information shared on a peer-to-peer network than to emails. Such information, once made available to others, no longer enjoys a reasonable expectation of privacy." Id.

As to the IP address information, the court agreed with the "myriad authorities affirm[ing] that 'subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.'" Id. at *7 (quoting United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008)). The court did not reach Morel's argument that Imgur uploaded the images

at "the behest of [NCMEC] and, thus, that Imgur's review amounted to a warrantless governmental search." Id. at *1.

As to the sufficiency of the state search warrant, the district court determined that although Detective Richard did not attach the alleged child pornography images to his affidavit, the warrant issued was valid as there was probable cause to believe that the images depicted girls under the age of eighteen. That was because Detective Richard's affidavit stated that he believed some of the girls depicted to be under ten years old and some under thirteen years old. Id. at *9. The district court found that Detective Richard's training and experience supported the reliability of his conclusion. Id.

II.

When reviewing the denial of motions to suppress, we review the district court's factual findings for clear error and its legal conclusions, including ultimate constitutional determinations, de novo. United States v. D'Andrea, 648 F.3d 1, 5 (1st Cir. 2011). We first consider Morel's argument that, contrary to the district court's conclusions, he had a reasonable expectation of privacy in his IP address information and in the images he uploaded to Imgur. We then turn to his argument that the warrant to search his computer was not supported by probable cause.

A. Whether Morel Had a Reasonable Expectation of Privacy in the IP Address or the Images

"The Supreme Court has set out a two-part test" for analyzing whether a defendant had a reasonable expectation of privacy: "first, whether the movant has exhibited an actual, subjective, expectation of privacy; and second, whether such subjective expectation is one that society is prepared to recognize as objectively reasonable." United States v. Rheault, 561 F.3d 55, 59 (1st Cir. 2009) (citing Smith v. Maryland, 442 U.S. 735, 740 (1979)).

"[T]he defendant carries the burden of making the threshold showing that he has 'a reasonable expectation of privacy in the area searched and in relation to the items seized.'" United States v. Stokes, 829 F.3d 47, 51 (1st Cir. 2016) (quoting United States v. Aguirre, 839 F.2d 854, 856 (1st Cir. 1988)). "Only then can he 'challenge the admissibility of evidence on fourth amendment grounds.'" Id. (quoting United States v. Gomez, 770 F.2d 251, 253 (1st Cir. 1985)). "This burden must be carried at the time of the pretrial hearing and on the record compiled at that hearing." Id. (quoting Aguirre, 839 F.2d at 856). The district court held that Morel had not met this burden. We agree.

Morel's primary argument is that Carpenter v. United States, 138 S. Ct. 2206 (2018), has effected a sea change in the law of reasonable expectation of privacy, and he is the beneficiary

of that change, both as to his IP address information and the images uploaded to Imgur. But Carpenter does not go so far; Morel's argument fails under Carpenter and under post-Carpenter caselaw.

Carpenter held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI [cell-site location information]."[7] 138 S. Ct. 2217. Carpenter did not announce a wholesale abandonment of the third-party doctrine. That doctrine states that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties . . . 'even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.'" Smith, 442 U.S. at 743-44 (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).

Carpenter declined to extend the third-party doctrine to the months of CSLI gathered by law enforcement in that case, 138 S. Ct. at 2216, because, as we recently explained:

> [G]iven the location information that CSLI conveyed and the fact that a cell phone user

[7] Carpenter expressly declined to decide "whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be," and concluded that "[i]t is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search." Carpenter, 138 S. Ct. at 2217 n.3.

> transmits it simply by possessing the cell phone, if the government could access the CSLI that it had acquired without a warrant in that case, then the result would be that "[o]nly the few without cell phones could escape" what would amount to "tireless and absolute surveillance."[8]

United States v. Hood, ___ F.3d ___, No. 18-1407, 2019 WL 1466943, at *3 (1st Cir. Apr. 3, 2019) (quoting Carpenter, 138 S. Ct. at 2218).

1. IP Address Information

Morel challenges the district court's decision that "subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation." Morel, 2017 WL 1376363, at *7 (quoting Perrine, 518 F.3d at 1204-05). Morel argues that this reasoning is no longer valid after Carpenter.

Our decision in Hood resolves this argument against Morel. 2019 WL 1466943, at *4. In Hood, the defendant was indicted on charges of transportation and receipt of child pornography, and moved to suppress evidence, including his IP address information,

[8] Other circuits have held in accord with Hood, 2019 WL 1466943 at *3-4, that Carpenter did not eliminate the third-party doctrine. United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018); Presley v. United States, 895 F.3d 1284, 1291 (11th Cir. 2018), cert. denied, No. 18-831, 2019 WL 1318587 (U.S. Mar. 25, 2019) (mem.). Carpenter's self-described "narrow" holding, 138 S. Ct. at 2220, does not support Morel's argument that he had a reasonable expectation of privacy in his IP address information or in the images uploaded to Imgur.

that was connected to information shared on a smartphone messaging application. Id. at *1-2. Like Morel, the defendant in Hood argued that under Carpenter, the third-party doctrine should not apply to IP address information that the government gathered from the smartphone messaging company.

Hood rejected this argument, because unlike CSLI information, IP address information on its own does not provide information concerning location. Id. at *4. "The IP address data is merely a string of numbers associated with a device that had, at one time, accessed a wireless network." Id. And, unlike CSLI, "an internet user generates the IP address data . . . only by making the affirmative decision to access a website or application." Id. Morel attempts to distinguish Hood on the ground that here, Morel "accessed the internet from a personal computer that he used in his family home." But Hood did not turn on the location from which the defendant accessed the internet. IP address information of the kind and amount collected here -- gathered from an internet company -- simply does not give rise to the concerns identified in Carpenter. As in Hood, Morel did not have a reasonable expectation of privacy in the IP address information that the government obtained from Imgur. It is that information which connected Morel to the uploaded images.

2. Images Uploaded to Imgur

Morel argues that he had a reasonable expectation of privacy in the images uploaded to Imgur. He disputes the district court's conclusions that the images uploaded to Imgur were publicly available, and that Morel did not take affirmative steps to maintain the privacy of the images he uploaded to Imgur. There was no clear error in the court's findings of fact, and we agree with its legal conclusions based on those facts.

Whether a defendant has a reasonable expectation of privacy is a fact-specific inquiry. Aguirre, 839 F.2d at 857. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." Katz v. United States, 389 U.S. 347, 351 (1967). "But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Id.

Factors especially relevant to determining whether one has a reasonable expectation of privacy include "ownership, possession and/or control; historical use of the property searched or the thing seized; ability to regulate access; the totality of the surrounding circumstances; the existence or nonexistence of a subjective anticipation of privacy; and the objective reasonableness of such an expectancy under the facts of a given case." Stokes, 829 F.3d at 53 (quoting Aguirre, 839 F.2d at 856–57).

The district court did not err in finding that "[n]o evidence suggests that Morel took affirmative steps to protect the images." Morel, 2017 WL 1376363, at *6. The record shows that Morel chose to upload the images to a website that makes it "impossible" to prevent third parties from accessing the images, whether the images are uploaded to "public" or "private" albums. Morel did not choose one of the more private website alternatives which exist. Viewing the Imgur images would not even require use of a password to gain access. And at least two third parties, the tipster and the NCMEC employee, did access the images Morel uploaded. An "NCMEC employee was able to open the gallery page and view the image thumbnails presented simply by entering the provided URL." Id.

Nor did the district court err in finding that the images were publicly available. The evidence was that "everyone in the world can see" images uploaded to public Imgur albums, and that those images are available on Imgur's public galleries. And even "private" Imgur albums can be seen by anyone who had the corresponding URL; there is no way to prevent third parties from accessing and sharing the URL.

On these facts, the classic third-party doctrine analysis prevents Morel from showing that he had a reasonable expectation of privacy in the images uploaded to Imgur. Morel argues that the district court did not find that Morel actually

shared any URLs with a third party. But this does not establish that Morel met his burden. He put on no evidence that he had not shared the URLs. And even if Morel had not shared the URLs, the evidence shows that he could not have prevented third parties from finding the images through a Google search or a lucky guess at the URL,[9] and third parties did access the images in this case.

Morel also relies on United States v. Mancini, 8 F.3d 104 (1st Cir. 1993), for the proposition that "shared access to a document does not prevent one from claiming Fourth Amendment protection in that document." Id. at 108. That case involved a town official sharing a single hard copy of an appointment calendar (kept in the town's archive attic) with his secretaries, who had a position of confidence with him. Id. at 108-09. This case is nothing like Mancini, and involved strangers, even random strangers, having access to images on a website.

B. Probable Cause Supporting the Search Warrant

Morel argues that the state warrant to search his computer was not supported by probable cause to believe that the girls depicted in the images were under the age of eighteen. The district court correctly held that the warrant was supported by probable cause. For the first time on appeal, Morel also argues

[9] Morel argues that it is highly unlikely that someone could have guessed or found the URLs at issue here, because they were composed of random numbers and letters, but he presented no evidence to this effect.

there was no probable cause to believe the girls depicted were "real," rather than virtual, children.

"The standard we apply in determining the sufficiency of an affidavit" supporting a state or federal warrant "is whether the 'totality of the circumstances' stated in the affidavit demonstrates probable cause to search either the premises or the person." United States v. Khounsavanh, 113 F.3d 279, 283 (1st Cir. 1997) (citing Illinois v. Gates, 462 U.S. 213, 238 (1983)). "Probable cause does not require either certainty or an unusually high degree of assurance. All that is needed is a 'reasonable likelihood' that incriminating evidence will turn up during a proposed search." United States v. Clark, 685 F.3d 72, 76 (1st Cir. 2012) (citation omitted) (quoting Valente v. Wallace, 332 F.3d 30, 32 (1st Cir. 2003)).

1. Whether There Was Probable Cause That the Images Depicted Girls Under the Age of Eighteen

Morel argues that in preparing the affidavit, Detective Richard failed to follow the "best practice" outlined in United States v. Syphers, 426 F.3d 461, 467 (1st Cir. 2005), and United States v. LaFortune, 520 F.3d 50, 58 (1st Cir. 2008), of attaching the suspected child pornography images to the warrant application or providing a sufficiently detailed description of the images.

LaFortune stated that the "best practice" language in Syphers was dicta, but that

> we now confirm [that dicta] as a holding essential to our decision here: The best practice is for an applicant seeking a warrant based on images of alleged child pornography to append the images or provide a sufficiently specific description of the images to enable the magistrate judge to determine independently whether they probably depict real children.

LaFortune, 520 F.3d at 58 (quoting Syphers, 426 F.3d at 467). "An officer who fails to follow this approach without good reason faces a substantial risk that the application for a warrant will not establish probable cause." Syphers, 426 F.3d at 467. Morel overreads LaFortune and Syphers. The risk described is not a certainty that there is no probable cause; it is the Fourth Amendment standard for probable cause which governs.

The "best practice" language in LaFortune is not applicable here in any event because the warrant was issued by a state court. The "best practice" judicial gloss cannot be imposed onto state courts. The question before us is simply whether the affidavit was supported by probable cause to believe the girls depicted in the images were under eighteen years old.

The warrant affidavit was sufficient to establish probable cause because it stated that Detective Richard believed that at least four of the girls depicted in three of the images were under the age of ten. An under-ten-year-old girl does not

look like, and is not mistaken for, an eighteen-year-old girl. While images of older minor girls may require more evidence of age, that is not true for images of girls aged under ten. The statement that the images depicted girls believed to be under the age of ten is not a boilerplate recitation "synonymous with the statutory definition of a minor."[10] Morel, 2017 WL 1376363, at *9.

It is highly improbable that Detective Richard, an officer experienced and trained in this field, would mistake an eighteen-year-old girl for an under-ten-year-old girl. The affidavit shows that Detective Richard was careful in assessing the ages of the different girls depicted, stating that he believed some to be under the age of ten, others to be under the age of thirteen, and still others to be of an "unknown age." Richard had sufficient experience to make such assessments. The affidavit stated that Detective Richard had been a police officer for over two decades, had received specialized training in child abuse and exploitation cases, had been on the Internet Crimes Against

[10] The district court noted that at a suppression hearing, "Det[ective] Richard confirmed what his words themselves conveyed: that he described the individuals as he did because they appeared, to him, to be prepubescent." Morel, 2017 WL 1376363, at *9. But our assessment of probable cause must be based on "information provided in the four corners of the affidavit supporting the warrant application." United States v. Vigeant, 176 F.3d 565, 569 (1st Cir. 1999). The affidavit in this case did not state that Detective Richard believed the females in the images were "prepubescent."

Children Task Force for nearly a decade, and had assisted in the execution of about fifty search warrants related to possession and distribution of child pornography. That training and experience likely informed his belief that the girls depicted in the images were under age eighteen.[11]

2. Whether There Was Probable Cause That the Images Depicted Real Children

Morel raises the issue of whether the girls depicted were real, as opposed to virtual, for the first time on appeal, so it is waived. See United States v. Oquendo-Rivas, 750 F.3d 12, 17 (1st Cir. 2014).

Morel argues that he did not waive this argument because, at a suppression hearing, the district court discussed caselaw stating that a magistrate judge must be able to independently determine whether the images "probably depict real children." See Syphers, 426 F.3d at 467; LaFortune, 520 F.3d at 58. This reference to caselaw does not preserve the issue. Morel also argues that this issue is "integral to the probable cause determination," and that the government could not have been surprised by it. We disagree. At the suppression hearings, the parties and the district court only considered the issue raised:

[11] Contrary to Morel's argument, Detective Richard was not required to apply the Tanner Scale to assess the ages of the girls in the images. United States v. Hilton is inapposite, because that case involved the government's burden of proof at trial. 386 F.3d 13, 15 (1st Cir. 2004).

whether the warrant was sufficient for probable cause as to the ages of the girls. This was not enough to apprise the district court of the issue of whether the girls were real. See McCoy v. Mass. Inst. of Tech., 950 F.2d 13, 22 (1st Cir. 1991) ("If claims are merely insinuated rather than actually articulated in the trial court, we will ordinarily refuse to deem them preserved for appellate review.").

III.

The district court's denial of Morel's suppression motions is affirmed.