

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.

UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

United States of America

v.

Civil No. 14-cr-148-JL
Opinion No. 2017 DNH 072

David Morel

OPINION AND ORDER

In advance of a trial on one count of possession of child pornography, see 18 U.S.C. § 2252(a)(4)(B), defendant David Morel Jr. filed a series of motions to suppress evidence. These motions turn on whether he had a reasonable expectation of privacy in images uploaded to the Internet and whether probable cause supported a warrant to search a computer for child pornography when the affiant police detective failed to attach known images of apparent child pornography to the warrant application.

By his first motion, Morel asked the court to suppress images of child pornography obtained from his computer and statements he made during a custodial interrogation, arguing that this evidence was obtained as the result of a warrantless search conducted by Imgur, a corporation, acting at the instigation of the National Center for Missing and Exploited

Children (NCMEC).¹ By his second motion, Morel sought to suppress the images obtained from his computer because, he argues, it was searched pursuant to a constitutionally-deficient warrant.² Morel also filed a third motion, seeking to suppress evidence obtained from what he contended was an unconstitutional warrantless arrest.³

After two evidentiary hearings, one on Morel's first motion to suppress and the other on Morel's second and third motions, the court denied all three motions.⁴ Morel subsequently conditionally pleaded guilty to one count of possessing child pornography in violation of [18 U.S.C. § 2252\(a\)\(4\)\(B\)](#), reserving the right to appeal the court's orders denying his first and second motions.⁵ See [Fed. R. Crim. P. 11\(a\)\(2\)](#). This order serves to set forth the bases for the court's denial of those two motions in greater detail. See, e.g., [United States v.](#)

¹ Morel filed a series of motions and supplemental motions in support of his arguments to this effect. See document nos. [24](#), [31](#), [33](#), [35](#), [40](#). The court considers this set of documents to constitute a single motion.

² Document no. [51](#).

³ Document no. [49](#).

⁴ See Orders of April 4, 2016, September 22, 2016, and September 30, 2016.

⁵ Because Morel thus waived his right to appeal the court's denial of his third motion to suppress, the court does not elaborate on its reasoning in this order.

Joubert, 980 F. Supp. 2d 53, 55 n.1 (D.N.H. 2014), aff'd, 778 F.3d 247 (1st Cir. 2015) (citing In re Mosley, 494 F.3d 1320, 1328 (11th Cir. 2007) (noting a district court's authority to later reduce its prior oral findings and rulings to writing)).

As explained below, Morel vigorously argues that Imgur reviewed his uploaded images at the behest of NECMEC and, thus, that Imgur's review amounted to a warrantless governmental search. Because Morel fails to establish that he possessed a reasonable expectation of privacy in the uploaded images, the court need not reach that question. The images, uploaded to the Internet, were not only accessible to but actually accessed by an anonymous tipster and NCMEC, strongly suggesting that Morel lacked any such expectation. As to his second motion, though the affiant failed to follow the "best practice" of attaching the known images of alleged child pornography to his affidavit in support of a warrant, his affidavit did not run afoul of the requirement that a judicial officer, not the investigating officer, make the probable cause determination because he sufficiently described the manner in which the images met the statutory requirements for child pornography. Accordingly, the court denied both motions.

I. Background

The court makes the following findings of fact based on the testimony and other evidence received at the suppression hearings.

A. NCMEC CyberTipline report

The National Center for Missing and Exploited Children (NCMEC) is a non-profit organization that works to reunite missing children with their families, reduce child sexual exploitation, and prevent child victimization. See [42 U.S.C. § 5771](#). To further that mission, NCMEC hosts a CyberTipline -- a website through which members of the public, law enforcement officials, and others can report child exploitation and child pornography by filling out a form on that website. [Id.](#) [§ 5773\(b\)\(1\)](#). The law obligates electronic service providers (ESPs) that "obtain[] actual knowledge of" child pornography to report that fact to NCMEC through the CyberTipline. [18 U.S.C. § 2258A\(a\)](#). Knowing and willful failure to do so is may be punished by a fine. [Id. § 2258A\(e\)](#). Upon receiving such a report, NCMEC must forward it to an appropriate federal law enforcement agency, and may forward it to an appropriate state or foreign law enforcement agency. [Id. § 2258A\(c\)](#).

The CyberTipline's online form contains several fields. While an individual or ESP reporting an instance of child pornography may fill out many or all of the fields available,

including contact information, only two fields are required: the date and time of the incident, and the substance of the report. An individual making a report can provide the web address of any files containing child pornography; he or she cannot, however, upload the image files. ESPs, on the other hand, can upload and attach images to those reports.

Irrespective of how many or which fields someone making a report fills out, NCMEC automatically captures the date and time that a report is submitted, as well as the IP address of the computer from which it was submitted.

On November 23, 2013, an unidentified individual reported instances of child pornography through the CyberTipline (report number 2195842), including a list of URLs of websites or images appearing to depict child pornography.⁶ This person provided no identifying information, but the CyberTipline captured his or her IP address and, via an automated process, populated the location associated with that IP address into the report. NCMEC's staff analysts then visited several of the reported URLs and annotated the report, indicating whether the visited URLs appeared to contain child pornography. In this report, one of the URLs led to a gallery of images hosted by an image-hosting

⁶ Hearing Ex. 2.

service called Imgur.⁷ The analyst obtained the URLs of specific images in the gallery that appeared to contain child pornography without clicking on the links thereto, and copied those URLs into the report.⁸

Once a day, NCMEC sends automated notices to ESPs summarizing instances of apparent child pornography reported from or found on their websites that day. On November 26, 2013, NCMEC sent such a notice to Imgur, indicating that images found at Imgur URLs appeared to contain child pornography, including images identified in report number 2195842.⁹ In this notice, NCMEC asked Imgur to “[p]lease review the reported URL to

⁷ Images hosted by Imgur are accessible either through links from the public gallery or by direct image link (URL). An image published to the public gallery is visible to anyone who visits Imgur’s website. An image published to a private gallery is still visible to everyone who possesses the direct image link. It is impossible to make an image uploaded to Imgur private such that it cannot be seen by any person, or can be seen only by the one who uploaded it.

Imgur does not actively search or use software to identify apparent child pornography uploaded by its users. According to testimony by its representative, Brianna Walker, however, when it receives reports of such images, it reviews the images and, if they appear to contain child pornography, reports them to NCMEC. It then deletes the images. This practice is reflected in Imgur’s terms of service, to which users must agree before uploading images. These terms of service indicate that, if Imgur finds illegal images, or images involving illegal activity, Imgur will report the user and delete the image. See Hearing Ex. J.

⁸ Hearing Ex. 2 at MOR01140.

⁹ Hearing Ex. 3.

determine if it contains content that violates federal and/or state law or your Terms of Service or Member Services Agreement.”¹⁰

NCMEC neither require ESPs to notify NCMEC whether they take action after receiving such a notice nor follows up with ESPs to see if they have done so. Nor does NCMEC instruct ESPs to report apparent child pornography found on such URLs. In this case, however, consistent with federal law, see 18 U.S.C. § 2258A(a), and with its own terms of service,¹¹ after receiving this notice, on November 26, 2013, Imgur filed three reports through the CyberTipline. These reports indicated that some of the URLs noted by NCMEC contained apparent child pornography (report nos. 2202631, 2202632, and 2202634).¹² As an ESP, Imgur was able to -- and did -- attach copies of the images to the reports. Imgur also provided the IP address of the computer from which the images were uploaded to Imgur’s servers,¹³ which was the same for all three images, as well as the date and time each image was uploaded. Using a publicly-available website,

¹⁰ Id.

¹¹ See Hearing Exs. J and M.

¹² Hearing Exs. B, C, and D.

¹³ NCMEC does not have the ability to obtain the uploading IP address by itself. It relies on ESPs to provide it. Not all ESPs do so.

NCMEC associated that IP address with a Comcast Cable subscriber in Derry, New Hampshire.¹⁴ Imgur then deleted the images from its server. On December 6, 2013, Imgur submitted three additional reports of apparent child pornography associated with the same IP address to NCMEC through the CyberTipline (report nos. 2217212, 2217316, and 2217317).¹⁵

Relying on Imgur's reports that the images contained apparent child pornography NCMEC notified and made Imgur's reports available to the New Hampshire Internet Crimes Against Children (ICAC) task force, which forwarded the reports to the Derry, New Hampshire police department.

B. Investigation

After receiving the six reports, Detective Kennedy Richard of the Derry Police Department reviewed the images attached thereto and characterized them as appearing to contain child pornography. He obtained a subpoena for Comcast's information concerning the owner of the identified IP address. On February 14, 2014, Comcast notified Det. Richard that the IP address in question belonged to a David Morel at an address on Pingree Hill Road in Derry, New Hampshire.

¹⁴ Hearing Ex. 4 at 2.

¹⁵ Hearing Exs. E, F, and G.

In the meantime, on February 1, 2014, defendant Morel reported that his laptop computer was stolen during a burglary from the loft above the garage at his parents' house at that address. The Derry Police Department recovered that computer and other stolen property a week later. During a visit to the police department, Morel identified the recovered computer as the one he had reported stolen. The computer remained in the police department's custody as evidence of the burglary.

Det. Richard subsequently spoke with the defendant's father, David Morel Sr.,¹⁶ who confirmed that defendant Morel lived at the Pingree Hill Road address in November, 2013, at the time the images were uploaded. David Morel Sr. also disavowed using the email address associated with the Comcast account connected to the identified IP address, and said he believed it was used by his son.

On April 16, 2014, Det. Richard obtained a warrant to search Morel's laptop computer that was in the police department's custody. In the affidavit supporting his application for the warrant, he described the six images attached to the NCMEC reports.¹⁷ He described three of the

¹⁶ To avoid any confusion, the court will refer to David Morel Sr. by his full name.

¹⁷ Det. Richard, in his affidavit, also stated that Imgur informed NCMEC that the images in question had been downloaded to a computer at the reported IP address. See First Mot. to

images as depicting females “believed to be” or who “appear[] to be under the age of 10.”¹⁸ The other three images depicted females “believed to be under the age of 13.”¹⁹ Though he described the apparently sexual nature of the photographs, he did not, in this application, physically describe the girls other than to state his belief that they were under the ages of 10 and 13.

Pursuant to the warrant issued on April 16, Det. Richard had a forensic copy made of Morel’s computer’s hard drive. He reviewed the contents of the hard drive a few days later and saw what he estimated to be approximately 200 videos and images depicting child pornography.

Supp. Ex. A (doc. no. [24-1](#)) at MOR00106. The weight of the evidence adduced at the hearing, including the NCMEC reports and testimony of Imgur’s representative, made clear that Imgur reported the images as being uploaded from that IP address, not downloaded to it. Morel did not seriously contest that fact. See Third Supplemental Mot. to Supp. (doc. no. [35](#)). Whether the images were uploaded from or downloaded to a given computer, the images must necessarily have existed on that computer at some point in time. Accordingly, to the extent that Morel briefly argues that this error in Det. Richard’s affidavit invalidates the resulting warrant, see Supplemental Mot. to Supp. (doc. no. [31](#)) at 6-7, the court concludes that this error did not render the affidavit “so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable,” thus rendering the evidence obtained pursuant to the warrant admissible under the good faith exception. [United States v. Capozzi, 347 F.3d 327, 332 \(1st Cir. 2003\)](#).

¹⁸ First Mot. to Supp. Ex. A (doc. no. [24-1](#)) at MOR00106-07.

¹⁹ [Id.](#)

On April 28, 2014, Morel was arrested on the charge of Attempted Possession of Child Sexual Abuse Images.²⁰ Det. Richard interviewed Morel at the Derry Police Department where, after receiving customary [Miranda](#) warnings and waiving his Fifth Amendment rights, Morel admitted to possessing child pornography on his computer.²¹ After the court denied his motions to suppress both the contents of his hard drive and his statement, Morel pled guilty to one count of possession of child pornography.

II. Analysis

Morel moves to suppress evidence of child pornography images obtained during a search of his computer's hard drive. In his first motion, he argues that the government would not have obtained this evidence -- as well as his confession, which he also seeks to suppress -- but for a warrantless search by Imgur of the images uploaded to Imgur from his IP address. In his second motion, Morel argues that probable cause did not

²⁰ Morel's third motion to suppress addressed the circumstances of that arrest. See Third Mot. to Supp. (doc. no. [50](#)). Because the court's order denying that motion is not subject to appeal, the court does not delve into those circumstances here.

²¹ Morel challenges the admissibility of his statement as fruit of the allegedly unconstitutional search of his uploaded images by Imgur. See Third Supplemental Mot. to Supp. (doc. no. [35](#)) at 1. He does not challenge the validity of his waiver of his rights under the Fifth Amendment.

support the April 16, 2014 warrant pursuant to which Det. Richard searched his computer's hard drive because Det. Richard's affidavit did not describe the images in such a way as to allow the issuing magistrate to conclude that the images met the statutory definition of child pornography. The court addresses each motion in turn.

A. First motion to suppress

The Fourth Amendment protects from violation the "right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." [U.S. Const. amend. IV](#). "A search within the meaning of the Fourth Amendment 'occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.'" [United States v. D'Andrea, 648 F.3d 1, 5-6 \(1st Cir. 2011\)](#) (quoting [Kyllo v. United States, 533 U.S. 27, 33 \(2001\)](#)). To determine whether an individual has a reasonable expectation of privacy in the place searched, the court asks, first, "whether the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy," and second, "whether the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable." [Smith v. Maryland, 442 U.S. 735, 740 \(1979\)](#) (internal quotations and citations omitted). Just as the defendant "has the burden of

establishing that his own Fourth Amendment rights were violated by the challenged search or seizure,” he also bears the “threshold burden . . . to prove that he had a legitimate expectation of privacy in ‘the place searched or the thing seized.’” [United States v. Rheault, 561 F.3d 55, 58-59 \(1st Cir. 2009\)](#) (internal quotations and citations omitted). Only after the defendant demonstrates a reasonable expectation of privacy does the court determine whether a governmental search violated that expectation.

Morel’s arguments in support of his first motion to suppress have evolved over the course of several rounds of briefing, presenting a moving target for the prosecution and the court.²² At the end of the day, that argument can be reduced to three points: (1) Morel had a reasonable expectation of privacy in images uploaded to Imgur’s server and in the IP address from which those images were uploaded; (2) Imgur’s review of those images and reporting of them and his IP address to NCMEC constituted a search that violated that expectation of privacy; and (3) that search amounted to a governmental search because Imgur, though not a governmental entity itself, conducted it at

²² The court does not intend this observation as any form of censure to defendant’s counsel. Morel’s evolving arguments reflected an evolving factual record, the result of a staggered dissemination of evidence by the prosecution.

the request of NCMEC. Because the court concludes that Morel lacked a reasonable expectation of privacy in the images that he uploaded to Imgur's servers and the IP address from which he uploaded them, the court need not reach the latter two questions.²³

1. Images uploaded to Imgur

An individual may have an expectation of privacy in certain information conveyed over the Internet, even though that information is stored on a third party's server, as the images were here. For example, acknowledging that individuals have a certain privacy interest in the content of emails, Congress, through the Electronic Communications Privacy Act ("ECPA"), barred ESPs from disclosing information about a customer's electronic communications to the government without a court order, warrant, or the customer's consent.²⁴ See [18 U.S.C.](#)

²³ Even were the court to reach the latter questions, the Court of Appeals has rejected Morel's argument that private image-hosting services act as government agents when they review users' accounts for child pornography and report any apparent child pornography to NCMEC pursuant to [18 U.S.C. § 2258A](#). See [United States v. Cameron, 699 F.3d 621, 638 \(1st Cir. 2012\)](#); see also [United States v. Keith, 980 F. Supp. 2d 33, 40-43 \(D. Mass. 2013\)](#) (AOL search of email attachment and subsequent report to NCMEC did not violate Fourth Amendment).

²⁴ There are also exceptions for providing, for example, a customer's name, address, and other information about the customer's subscription (but not the content of electronic communications) to a governmental entity in response to an administrative or grand jury subpoena. [18 U.S.C. § 2703\(c\)\(2\)](#).

[§§ 2702, 2703](#). Courts have similarly acknowledged such privacy interests, analogizing emails in the hands of a service provider to unopened packages in the hands of a common carrier like Federal Express or UPS. E.g., [United States v. Warshak, 631 F.3d 266, 288 \(6th Cir. 2010\)](#) (holding in the Fourth Amendment context that “a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP”); see also [Keith, 980 F. Supp. 2d at 39-40](#) (analogizing the content of emails to the contents of a conversation held over a telephone line or a sealed envelope).

Morel’s emails are not implicated here.²⁵ He argues, rather, that the same principles protecting emails apply to images uploaded to Imgur’s servers and the IP address from which he uploaded them.²⁶ But that analogy does not hold. Here, the evidence suggests that any images uploaded to Imgur’s servers were publicly available. As Imgur’s representative testified, there is no way to render an image entirely private on Imgur. At best, a user can decline to share the image’s URL, thus not

²⁵ In his original motion, Morel argued that the government had searched his emails. See Mot. to Supp. (doc. no. [24](#)). He later conceded that his emails were never subject to a search. See Third Supplemental Mot. to Supp. (doc. no. [35](#)) at 1.

²⁶ See [id.](#) at 1.

affirmatively inviting others to view the image. Such images are still able to be found by the public at large through search engines, reverse image searches, or even by a lucky guess at the URL.

An individual who places a file on the Internet, without taking affirmative steps to protect the information it contains, cannot reasonably expect it to remain private. See [D'Andrea, 648 F. 3d at 8](#) ("It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information." (quoting [United States v. Jacobsen, 466 U.S. 109, 117 \(1984\)](#))); see also [United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 \(D.P.R. 2002\)](#), rev'd on other grounds, [90 Fed. Appx. 3 \(1st Cir. 2004\)](#) ("[I]t strikes the Court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably public medium, such as the Internet, without taking any measures to protect the information."); cf. [Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369, 373 \(D.N.J. 2012\)](#) (expectation of privacy in Facebook comments only where plaintiff restricted access thereto). No evidence suggests that Morel took affirmative steps to protect the images. To the contrary, the evidence indicates that the uploaded images were generally available to

-- and findable and viewable by -- the public at large. Specifically, the anonymous tipster who submitted the initial report to the NCMEC CyberTipline appears able to have accessed the images, so as to determine their content and suggest to NCMEC that they contained child pornography.²⁷ Similarly, a NCMEC employee was able to open the gallery page and view the image thumbnails presented simply by entering the provided URL. In this sense, 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. See, e.g., United States v. Ladeau, No. CRIM 09-40021-FDS, 2010 WL 1427523, at *1-5 (D. Mass. Apr. 7, 2010) (an individual using peer-to-peer networking software has no reasonable expectation of privacy in the information shared on that network); United States v. Norman, 448 F. App'x 895, 897 (11th Cir. 2011) (same); United States v.

²⁷ Morel has not argued any law enforcement misconduct in this action, such as law enforcement posting as an anonymous tipster, or that the tipster's access to the images violated the Fourth Amendment.

[Sawyer, 786 F. Supp. 2d 1352, 1355-56 \(N.D. Ohio 2011\)](#) (same, collecting cases).

Nor do Imgur's terms of service in and of themselves, as Morel argues, create an expectation of privacy in uploaded images.²⁸ Those terms state:

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, etc., then it may end up in the gallery.²⁹

As such, they appear to grant the user a measure of control over when, how, and with whom to share the URLs of images hosted on Imgur's servers. Any expectation of privacy they may purport to create is undermined on two fronts. First, they speak entirely of sharing: a user can share the images publicly, via social media, or with his or her friends alone. They do not, on their face, appear to contemplate purely private storage. And even if a user exercises some of that measure of control by choosing with whom to share the URLs, once those URLs have been shared with any third party, any potential expectation of privacy evaporates because the user lacks control over what the third party will do with them. See [United States v. Lifshitz, 369](#)

²⁸ See Supplemental Mot. to Supp. (doc. no. [31](#)) at 4-5.

²⁹ Ex M at 2.

F.3d 173, 190 (2d Cir. 2004) (no “expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient”); In re United States, 665 F. Supp. 2d 1210, 1223 (D. Or. 2009) (analogizing received emails to private documents left at one’s mother’s house). Second, Imgur’s terms of service go on to explain:

[I]f you do anything illegal, in addition to any other legal rights we may have, we will ban you[,] . . . delete all of your images, report you to the authorities if necessary, and prevent you from viewing any images hosted on Imgur.com. We mean it.³⁰

Such a warning intimates that Imgur, at least, contemplates its own access to images placed on its servers, regardless of a user’s consent to that access, in the event of, among other things, illegal activity.

Absent any indication that Morel took any affirmative steps to protect or prevent others from accessing images uploaded to Imgur’s servers, and in light of evidence demonstrating that an anonymous individual and NCMEC accessed the images that Morel made available through Imgur, the court concludes that Morel has failed to demonstrate a reasonable expectation of privacy in the uploaded images, subjective or objective.

³⁰ Hearing Ex. M.

2. IP address

Morel also suggests, and at the suppression hearing his counsel argued, that Imgur also acted improperly in providing NCMEC with the IP address from which he uploaded the images.³¹ Though he does not further develop this argument, the court notes that myriad authorities affirm that “subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation.” [United States v. Perrine, 518 F.3d 1196, 1204-05 \(10th Cir. 2008\)](#) (collecting cases). Such subscriber information includes, among other things, a subscriber’s name, address, and IP address. [Id. at 1203-04](#). Similarly, though the ECPA bars ESPs from disclosing information about a customer’s electronic communications to the government without a court order, warrant, or the customer’s consent, [see 18 U.S.C. §§ 2702, 2703](#), Congress explicitly carved out an exception to those privacy rules that permits ESPs to divulge a customer’s records (such as his IP address) “to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section [2258A](#).” [18 U.S.C. § 2702\(b\)\(6\), \(c\)\(5\)](#). As such, the court declines to

³¹ [See](#) Second Supp. Mot. (doc. no. [33](#)) at 5 (“Imgur then reported the results of the search, most notably the IP address, to NCMEC.”).

conclude that Morel had a privacy interest in the IP address that Imgur submitted to NCMEC.

Having concluded that Morel has not carried his burden of demonstrating that he had a reasonable expectation of privacy in images uploaded to Imgur's servers and his IP address, the court need not reach the question of whether Imgur acted as a "government agent" in reviewing Morel's images and reporting them to NCMEC. See [Cameron, 699 F.3d at 637-38](#) (applying the three-part test for "determining whether a private party has acted as a government agent" such that the private party's search implicates the Fourth Amendment). Because even "[o]fficial conduct that does not 'compromise any legitimate interest in privacy' is not a search subject to the Fourth Amendment," [Illinois v. Caballes, 543 U.S. 405, 409 \(2005\)](#) (quoting [Jacobsen, 466 U.S. at 123](#)), the court denies Morel's first motion to suppress.

B. Second motion to suppress

Morel next moves to suppress evidence of apparent child pornography found on the computer recovered by the Derry Police Department following his burglary complaint on the grounds that (1) the April 16, 2014 warrant pursuant to which that computer was searched was not supported by probable cause, and (2) the Derry Police Department unduly delayed obtaining the warrant.

Finding neither of these arguments persuasive, the court denies Morel's second motion to dismiss.

1. Probable cause

The Fourth Amendment provides that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." [U.S. Const. amend. IV](#). "Probable cause for a warrant based on an affidavit exists where information in the affidavit reveals a fair probability that contraband or evidence of a crime will be found in a particular place. Probability is the touchstone of this inquiry." [United States v. Syphers, 426 F.3d 461, 464 \(1st Cir. 2005\)](#) (internal quotations and citations omitted). "The standard applied in determining the sufficiency of an affidavit is a 'totality of the circumstances' test." [Id., 426 F.3d at 465](#) (quoting [United States v. Garcia, 983 F.2d 1160, 1167 \(1st Cir. 1993\)](#)). "[P]robable cause to issue a warrant must be assessed by a judicial officer, not an investigating agent. This judicial determination is particularly important in child pornography cases, where the existence of criminal conduct often depends solely on the nature of the pictures." [United States v. Brunette, 256 F.3d 14, 18 \(1st Cir. 2001\)](#).

Morel argues that Det. Richard's affidavit runs afoul of the requirement that a judicial officer, not the investigating agent, make the probable cause determination.³² In his affidavit in support of the April 16 warrant, Det. Richard indicated that he had reviewed the six images attached to the NCMEC CyberTipline reports forwarded to him. He described those images as depicting females who were naked, or naked from the waist down, one of whom "appears to be under the age of 10," three of whom he "believed to be under the age of 10," and four of whom he "believed to be under the age of 13."³³ He also described the apparently lascivious positions in which those individuals were posed. He did not, however, attach the images themselves to his affidavit.

Morel argues that this affidavit failed to provide probable cause that the images satisfied the first element of the offense of possessing child pornography -- that the images depict minors, which are defined as "any person under the age of eighteen years."³⁴ See [18 U.S.C. §§ 2252\(a\)\(4\)\(B\)\(i\), 2256\(1\)](#). "The best practice is for an applicant seeking a warrant based

³² See Mem. in Support of Second Mot. to Supp. (doc. no. [51-1](#)) at 3-4.

³³ Second Mot. to Supp. Ex. 1 (doc. no. [51-2](#)) at MOR00106-07.

³⁴ Morel does not challenge the sufficiency of Det. Richard's description of the sexual activity depicted in the images.

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.” [Syphers, 426 F.3d at 467](#); [United States v. LaFortune, 520 F.3d 50, 58 \(1st Cir. 2008\)](#) (confirming “the best practice dicta in [Syphers](#) . . . as a holding essential to our decision here” and affirming probable cause where officers attached images to affidavit). Det. Richard did not attach the images to his affidavit. The question, therefore, is whether his description of the individuals depicted is “sufficiently specific” for the reviewing magistrate to determine that the images depicted minors.

The court in [Syphers](#) was presented with a similar question. There, the affiant indicated that videos and/or photographs depicted “female minors that appeared to be younger than 16 years old,” or “appear[ed] to be under the age of 18 years of age.” [Syphers, 426 F.3d at 464](#). The Court of Appeals noted that “the application did not include the images seized previously or provide any detailed description of the physiological features of the persons depicted in those images (i.e., by describing body proportion, growth and development),” rendering the case “a tough call.” [Id. at 466](#). It did not “decide under the totality of the circumstances whether probable

cause supported the . . . warrant” despite that omission, however, finding that the good faith exception to the exclusionary rule saved the warrant, which issued five months before the Supreme Court, in [Ashcroft v. Free Speech Coalition](#), [535 U.S. 234, 256 \(2002\)](#), “held that the prohibition on child pornography that only ‘appears to be[] of a minor’ engaging in sexually explicit conduct was overbroad and violated the First Amendment.” [Syphers](#), [426 F.3d at 465, 467-68](#).

To be sure, Det. Richard’s failure to either (a) present the images to the magistrate or (b) describe the physiological characteristics that led him to conclude that the young girls depicted were under ages ten and thirteen, respectively, make this court’s evaluation of the warrant more difficult than it would have been had he used the best practices as outlined by [Syphers](#) and [LaFortune](#). But this case does not present the same “tough call” as [Syphers](#). In his affidavit, the agent in [Syphers](#) stated only that he believed that the individuals depicted were under 18 or 16 years of age -- a recitation equivalent, or almost equivalent, to the bare assertion, rejected in [Free Speech Coalition](#), that the individual “appears to be a minor.” That affidavit, the Court of Appeals observed, lacked any justification for that assertion. [Syphers](#), [426 F.3d at 466](#).

The situation here is somewhat different because Det. Richard described the individuals in the images as appearing to

be under 13 or 10 years of age -- ages that, unlike "under 18 years of age," are not synonymous with the statutory definition of a minor. At the hearing, Det. Richard confirmed what his words themselves conveyed: that he described the individuals as he did because they appeared, to him, to be prepubescent. His experience, which he described in his affidavit and which includes his training and participation in the Internet Crimes Against Children Task Force and his 23 years with the Derry Police Department, primarily in the juvenile division handling sexual assault and molestation cases, supports the reliability of his conclusion. See [United States v. Getzel, 2002 DNH 170, 10-12](#) (citing, among other things, agent's experience in finding that affidavit describing images as depicting "minor" children and "prepubescent" children supported by probable cause).

Describing children as "prepubescent" or "early pubescent" can establish probable cause that the images in question depict child pornography. Cf. [United States v. Edwards, No. 12-CR-43-JD, 2012 WL 4076169, at *1-2 \(D.N.H. Sept. 12, 2012\)](#) (probable cause existed where affidavit described images as depicting "girls who appeared to [sic] underage, in that they appeared to be prepubescent" and "young girls who had underdeveloped or no breasts and no pubic hair, in explicit poses"); [United States v. Barker, No. 5:11-CR-73, 2012 WL 12543, at *6 \(D. Vt. Jan. 3, 2012\)](#) (probable cause existed where affidavit described

purported minors as “prepubescent,” “early pubescent,” and “early adolescent”). Such terms clearly need no elaboration because they connote physical attributes (such as under- or non-developed sex organs or breasts, lack of pubic hair, and juvenile muscle development) consistent with an age well under the age of majority. In the same way that describing those depicted as “prepubescent” would not implicate the concerns expressed in [Syphers](#) and [LaFortune](#), neither would describing them as “under 10” or “under 13.” Accordingly, while following the “best practice” prescribed by the Court of Appeals would have been preferable, the search warrant was supported by sufficient evidence that the individuals depicted were minors.

2. Delay

“[A] seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment's prohibition on ‘unreasonable seizures.’” [Jacobsen, 466 U.S. at 124](#). Thus, “even a seizure based on probable cause is unconstitutional if police act with unreasonable delay in securing a warrant.” [United States v. Martin, 157 F.3d 46, 54 \(2d Cir. 1998\)](#).

Morel argues that “the length of the delay between the time the police obtained the computer and the information in their

supporting affidavit until the time they actually applied for a search warrant” requires exclusion of the evidence obtained through that warrant, including the contents of the computer’s hard drive.³⁵ Det. Richard received the subpoena response from Comcast associating the IP address in the NCMEC reports with David Morel of Pingree Hill Road in Derry, New Hampshire, on February 14, 2014. He did not seek a warrant to search Morel’s computer until some two months later, on April 16. Morel argues that this two-month delay “is presumptively too long and should result in suppression of any evidence obtained with the warrant.”³⁶

Observing that an individual’s computer likely contains items of a personal nature, such as photographs, emails, financial information, etc., the Eleventh Circuit Court of Appeals concluded “the detention of the [defendant’s] hard drive for over three weeks before a warrant was sought constitute[d] a significant interference with [his] possessory interest” in that hard drive. [United States v. Mitchell, 565 F.3d 1347, 1351 \(11th Cir. 2009\)](#). That unjustified delay was unreasonable, the court concluded, because the agent made no effort to obtain a

³⁵ [See](#) Mem. in Support of Second Mot. to Supp. (doc. no. [51-1](#)) at 4.

³⁶ [Id.](#)

warrant during that period; and the unreasonable delay warranted granting the defendant's motion to suppress. [Id. at 1353](#).

While Det. Richard could have been more diligent in following up on the investigation,³⁷ Morel's reliance on [Mitchell](#) is misplaced here because there is no evidence that the delay in obtaining the April 16 warrant interfered with Morel's possessory interest in his computer. The computer was already in the custody of the Derry Police as evidence of the burglary reported by Morel when Det. Richard received the subpoena response from Comcast on February 14.³⁸ Morel visited the police

³⁷ He offered no explanation, for example, as to why he did not contact David Morel Sr. to determine which David Morel may have been associated with the Comcast account until March 18 and, having obtained that information, waited yet another month before obtaining the warrant. When pressed, he cited only vacations and his case load as the probable reasons for the delay -- reasons akin to those that the court in [Mitchell](#) found unpersuasive. See [id. at 1352](#) (finding that agent's attendance at a two-week training program provided no excuse for delay in applying for warrant).

³⁸ Morel characterizes the computer as having been "seized without a warrant during the burglary investigation" Mem. in Support of Second Mot. to Suppress (doc. no. [51-1](#)) at 4. If this assertion is serious, it is insufficiently developed to warrant analysis. See [United States v. Zannino, 895 F.2d 1, 17 \(1st Cir. 1990\)](#) (insufficiently developed arguments are waived). Morel does not explain whether he had a legitimate expectation of privacy in the location from which the stolen laptop was recovered so as to have standing to challenge the lack of a warrant to recover it. See [United States v. Aguirre, 839 F.2d 854, 856 \(1st Cir. 1988\)](#) (defendant without privacy expectation in area searched lacks standing to challenge warrantless search).

department to identify it as his after it was recovered, but there is no evidence -- or even argument -- that he asked to have it returned to him during that time, or even how long the police planned to keep custody of it. To the contrary, he was informed that the police department would hold it pending the conclusion of its burglary investigation. Accordingly, the court declines to find that unreasonable delay in securing the warrant rendered the seizure and search of Morel's laptop unconstitutional.

III. Conclusion

Because Morel lacked a reasonable expectation of privacy in images stored on Imgur's servers and the application for the warrant to search his computer, resulting from the discovery of those images, established probable cause to believe that evidence of a crime would be found on it, the court DENIED Morel's first and second motions to suppress the evidence found there or Morel's custodial statements.³⁹

SO ORDERED.



Joseph N. Laplante
United States District Judge

Dated: April 14, 2017

³⁹ Document nos. [24](#), [31](#), [33](#), [35](#), and [51](#).

cc: Helen W. Fitzgibbon, AUSA
Shane Kelbley, AUSA
Philip H. Utter, Esq.

UNITED STATES DISTRICT COURT

JUN 30 2017

District of New Hampshire

FILED

UNITED STATES OF AMERICA

v.

David Morel, Jr.

JUDGMENT IN A CRIMINAL CASE

Case Number: 14-cr-148-01-JL

USM Number: 13762-049

Philip H. Utter, Esq.

Defendant's Attorney

THE DEFENDANT:

pleaded guilty to count(s) Count 1 of the Indictment

pleaded nolo contendere to count(s) _____
which was accepted by the court.

was found guilty on count(s) _____
after a plea of not guilty.

The defendant is adjudicated guilty of these offenses:

Title & Section	Nature of Offense	Offense Ended	Count
18 U.S.C. § 2252(a)(4) (B)	Possession of Child Pornography	4-28-2014	1

--	--	--	--

The defendant is sentenced as provided in pages 1 through 7 of this judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

The defendant has been found not guilty on count(s) _____

Count(s) _____ is are dismissed on the motion of the United States.

Count(s)

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid. If ordered to pay restitution, the defendant must notify the court and United States attorney of material changes in economic circumstances.

6/27/2017

Date of Imposition of Judgment

Signature of Judge

Joseph N. Laplante U.S. Chief Judge

Name and Title of Judge

Date

6/30/17

DEFENDANT: David Morel, Jr.
CASE NUMBER: 14-cr-148-01-JL

IMPRISONMENT

The defendant is hereby committed to the custody of the Federal Bureau of Prisons to be imprisoned for a total term of:
70 months.

The court makes the following recommendations to the Bureau of Prisons:

That the defendant be designated to FCI Danbury.

That the defendant participate in a sex offender treatment program while incarcerated, if eligible.

The defendant is remanded to the custody of the United States Marshal.

The defendant shall surrender to the United States Marshal for this district:

at _____ a.m. p.m. on _____ .

as notified by the United States Marshal.

The defendant shall surrender for service of sentence at the institution designated by the Bureau of Prisons:

before 2 p.m. on _____ .

as notified by the United States Marshal.

as notified by the Probation or Pretrial Services Office.

RETURN

I have executed this judgment as follows:

Defendant delivered on _____ to _____
at _____ , with a certified copy of this judgment.

UNITED STATES MARSHAL

By _____
DEPUTY UNITED STATES MARSHAL

DEFENDANT: David Morel, Jr.
CASE NUMBER: 14-cr-148-01-JL

SUPERVISED RELEASE

Upon release from imprisonment, you will be on supervised release for a term of :
10 years.

MANDATORY CONDITIONS

1. You must not commit another federal, state or local crime.
2. You must not unlawfully possess a controlled substance.
3. You must refrain from any unlawful use of a controlled substance. You must submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.
 The above drug testing condition is suspended, based on the court's determination that you pose a low risk of future substance abuse. *(Check, if applicable.)*
4. You must cooperate in the collection of DNA as directed by the probation officer. *(Check, if applicable.)*
5. You must comply with the requirements of the Sex Offender Registration and Notification Act (42 U.S.C. § 16901, *et seq.*) as directed by the probation officer, the Bureau of Prisons, or any state sex offender registration agency in which you reside, work, are a student, or were convicted of a qualifying offense. *(Check, if applicable.)*
6. You must participate in an approved program for domestic violence. *(Check, if applicable.)*

You must comply with the standard conditions that have been adopted by this court as well as with any other conditions on the attached page.

DEFENDANT: David Morel, Jr.
CASE NUMBER: 14-cr-148-01-JL

SPECIAL CONDITIONS OF SUPERVISION

1. You must participate in a sex offense-specific assessment. You must pay the costs of the assessment to the extent you are able as determined by the probation officer.
2. You must participate in a sex offense-specific treatment program and follow the rules and regulations of that program. The probation officer will supervise your participation in the program. You must pay the costs of the program to the extent you are able as determined by the probation officer.
3. You must participate in the plethysmograph testing as party of the required participation in a sex offense-specific assessment and/or treatment.
4. You must submit to periodic polygraph testing at the discretion of the probation officer as a means to ensure that you are in compliance with the requirements of your supervision or treatment program.
5. You must not have direct contact with any child you know or reasonably should know to be under the age of eighteen, not including your own child, without the permission of the probation officer. If you do have any direct contact with any child you know or reasonably should know to be under the age of eighteen, not including your child, without the permission of the probation officer, you must report this contact to the probation officer within 24 hours. Direct contact includes written communication, in-person communication, or physical contact. Direct contact does not include incidental contact during ordinary daily activities in public places.
6. You must not view or possess any "visual depiction" (as defined in 18 U.S.C. § 2256), including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of "sexually explicit conduct" (as defined in 18 U.S.C. § 2256) that would compromise your sex offense-specific treatment.
7. You must not access the Internet except for reasons approved by the probation officer.
8. You must submit your computers (as defined in 18 U.S.C. § 1030[e][1]) or other electronic communications or data storage devices or media, to a search.
9. You must allow the probation officer to install computer monitoring software on any computer (as defined in 18 U.S.C. § 1030[3][1]).
10. To ensure compliance with the computer monitoring condition, you must allow the probation officer to conduct initial and periodic unannounced searches of any computers (as defined in 18 U.S.C. § 1030[3][1]) subject to computer monitoring. These searches shall be conducted for the purposes of determining whether the computer contains any prohibited data prior to installation of the monitoring software; to determine whether the monitoring software is functioning effectively after its installation; and to determine whether there have been attempts to circumvent the monitoring software after its installation. You must warn any other people who use these computers that the computers may be subject to searches pursuant to this condition.
11. You must submit your person, property, house, residence, vehicle, papers, computers (as defined in 18 U.S.C. § 1030 [3][1]), other electronic communications or data storage devices or media, or office, to a search conducted by a U.S. probation officer. Failure to submit to a search may be grounds for revocation. You must warn any other residents that the premises may be subject to searches pursuant to this condition. The probation officer may conduct a search under this condition only when reasonable suspicion exists that you have violated a condition of supervision and that the areas to be searched contain evidence of this violation. Any search must be conducted at a reasonable time and in a reasonable manner.

DEFENDANT: David Morel, Jr.
CASE NUMBER: 14-cr-148-01-JL

SPECIAL CONDITIONS OF SUPERVISION

12. You must participate in a substance abuse treatment program and follow the rules and regulations of that program. The probation officer will supervise your participation in the program (provider, location, modality, duration, intensity, etc.). You must pay for the cost of treatment to extent you are able, as determined by the probation officer.
13. You must submit to substance abuse testing to determine if you have used a prohibited substance. You must pay the costs of the testing if you are able as determined by the supervising officer. You must not attempt to obstruct or tamper with the testing methods.
14. You must not knowingly purchase, possess, distribute, administer, or otherwise use any psychoactive substances (e.g., synthetic marijuana, bath salts, etc.) that impair a person's physical or mental functioning, whether or not intended for human consumption, except with the prior approval of the probation officer.
15. You must not use or possess any controlled substances without a valid prescription. If you do have a valid prescription, you must disclose the prescription information to the probation officer and follow the instructions on the prescription.

DEFENDANT: David Morel, Jr.
CASE NUMBER: 14-cr-148-01-JL

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments on Sheet 6.

	<u>Assessment</u>	<u>JVTA Assessment *</u>	<u>Fine</u>	<u>Restitution</u>
TOTALS	\$ 100.00	\$	\$	\$

The determination of restitution is deferred until _____. An *Amended Judgment in a Criminal Case (AO 245C)* will be entered after such determination.

The defendant must make restitution (including community restitution) to the following payees in the amount listed below.

If the defendant makes a partial payment, each payee shall receive an approximately proportioned payment, unless specified otherwise in the priority order or percentage payment column below. However, pursuant to 18 U.S.C. § 3664(i), all nonfederal victims must be paid before the United States is paid.

<u>Name of Payee</u>	<u>Total Loss**</u>	<u>Restitution Ordered</u>	<u>Priority or Percentage</u>

TOTALS	\$	<u>0.00</u>	\$	<u>0.00</u>
---------------	----	-------------	----	-------------

Restitution amount ordered pursuant to plea agreement \$ _____

The defendant must pay interest on restitution and a fine of more than \$2,500, unless the restitution or fine is paid in full before the fifteenth day after the date of the judgment, pursuant to 18 U.S.C. § 3612(f). All of the payment options on Sheet 6 may be subject to penalties for delinquency and default, pursuant to 18 U.S.C. § 3612(g).

The court determined that the defendant does not have the ability to pay interest and it is ordered that:

the interest requirement is waived for the fine restitution.

the interest requirement for the fine restitution is modified as follows:

* Justice for Victims of Trafficking Act of 2015, Pub. L. No. 114-22.

** Findings for the total amount of losses are required under Chapters 109A, 110, 110A, and 113A of Title 18 for offenses committed on or after September 13, 1994, but before April 23, 1996.

DEFENDANT: David Morel, Jr.
CASE NUMBER: 14-cr-148-01-JL

SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties is due as follows:

- A Lump sum payment of \$ 100.00 due immediately, balance due
 - not later than _____, or
 - in accordance C, D, E, or F below; or
- B Payment to begin immediately (may be combined with C, D, or F below); or
- C Payment in equal _____ (e.g., weekly, monthly, quarterly) installments of \$ _____ over a period of _____ (e.g., months or years), to commence _____ (e.g., 30 or 60 days) after the date of this judgment; or
- D Payment in equal _____ (e.g., weekly, monthly, quarterly) installments of \$ _____ over a period of _____ (e.g., months or years), to commence _____ (e.g., 30 or 60 days) after release from imprisonment to a term of supervision; or
- E Payment during the term of supervised release will commence within _____ (e.g., 30 or 60 days) after release from imprisonment. The court will set the payment plan based on an assessment of the defendant's ability to pay at that time; or
- F Special instructions regarding the payment of criminal monetary penalties:

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during the period of imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program, are made to the Clerk, U.S. District Court, 55 Pleasant Street, Room 110, Concord, N.H. 03301. Personal checks are not accepted.

The defendant shall receive credit for all payments previously made toward any criminal monetary penalties imposed.

Joint and Several

Defendant and Co-Defendant Names and Case Numbers (including defendant number), Total Amount, Joint and Several Amount, and corresponding payee, if appropriate.

- The defendant shall pay the cost of prosecution.
- The defendant shall pay the following court cost(s):
- The defendant shall forfeit the defendant's interest in the following property to the United States:

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) fine principal, (5) fine interest, (6) community restitution, (7) JVTA assessment, (8) penalties, and (9) costs, including cost of prosecution and court costs.