UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

United States of America

v.

David Morel

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

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, Hew 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.