RECOMMENDED FOR FULL-TEXT PUBLICATION
Pursuant to Sixth Circuit I.O.P. 32.1(b)

File Name: 18a0062p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

DEREK MICHAEL TAGG,

Defendant-Appellee.

No. 17-1777

Appeal from the United States District Court
for the Eastern District of Michigan at Detroit.
No. 2:16-cr-20597-1—Paul D. Borman, District Judge.

Argued: March 7, 2018

Decided and Filed: March 27, 2018

Before: COOK, McKEAGUE, and STRANCH, Circuit Judges.

COUNSEL

ARGUED: Mark J. Chasteen, UNITED STATES ATTORNEY'S OFFICE, Detroit, Michigan, for Appellant. Benton C. Martin, FEDERAL DEFENDER OFFICE, Detroit, Michigan, for Appellee. **ON BRIEF:** Mark J. Chasteen, UNITED STATES ATTORNEY'S OFFICE, Detroit, Michigan, for Appellant. Benton C. Martin, FEDERAL DEFENDER OFFICE, Detroit, Michigan, for Appellee.

McKEAGUE, J., delivered the opinion of the court in which COOK and STRANCH, JJ., joined. STRANCH, J. (pg. 16), delivered a separate concurring opinion.

OPINION

McKEAGUE, Circuit Judge. In September 2015, police executed a warrant at Derek Tagg's residence, searching for child pornography. They found plenty of it—over 20,000 files, all stored on Tagg's computer. The search warrant was based primarily on digital evidence from an FBI operation showing that Tagg had spent over five hours browsing a website ("Playpen") that obviously contained child pornography. The district court found that the police lacked probable cause to search Tagg's house because the search warrant did not state that Tagg actually viewed any illegal images while on the site. Further, the court held that no reasonable officer would have relied on the warrant, and therefore suppressed all the evidence seized from Tagg's home. Because the warrant was supported by probable cause, we **REVERSE** the order granting the motion to suppress and **REMAND** the case for proceedings not inconsistent with this opinion.

I

This case arises out of federal and state investigations into child exploitation on the "dark web." The "dark web" is a sophisticated, anonymous internet network used both by criminals and by other individuals who, for whatever reason, do not want to be identified.

A

Until it was shut down by the FBI, Playpen operated a secret website on the "dark web." Although we think of websites as "out there" in the ether, the physical location of an ordinary website is on a computer programmed to permit access by anyone connected to the internet. Typical internet users access websites by searching for subjects through search engines (e.g., Google) in widely available web browsers (e.g., Mozilla Firefox), just like the ordinary shopper can walk into a store and look for signs indicating the location of the goods they desire. Clandestine websites like Playpen, however, sometimes require a "mask" before you can enter the computer(s) housing them. In this case, that "mask" is a web browser called "Tor," which hides your online "face" from other people on the internet.

Your online "face" is known as an "IP address," a unique number assigned to every computer connected to the internet. To hide your identity, Tor effectively masks your IP address so that the people operating the website's physical computers cannot trace your IP address back to your personal identity or your residence. Because this makes it difficult for anonymous websites to track customer preferences or allow users to interact with one another, websites like Playpen require you to create an identifying "pseudonym" when you enter the website. Thus, Playpen knows what each user likes and what it has looked at, but it cannot discern who the user is outside the confines of the website.

Further, Tor can also hide a website from all search engines entirely. In other words, a website operating on the Tor network can require you to know the *exact* combination of letters and numbers comprising the website's URL[1] before permitting you to see its content. And unlike intuitive URLs like *cnn.com* or *nytimes.com*, the URL of a secret Tor website like Playpen is randomized—for example, *upf45jv3bziuctml.onion*. Absent some statistically impossible stroke of luck, a site like Playpen is "an island that cannot be found, except by those who already know where it is." To access such a website, a newcomer must generally befriend someone who knows the URL, usually the website owner or another frequent user.

But just like in real life, nothing on the internet can be kept totally secret. Police or malicious website owners have discovered ways to work around Tor's "mask" and identify the people who visit a website. This is done by embedding software in the fabric of the website, which creates a digital "fingerprint"[2] identifying each user's IP address. Police can then link the

---

[1] "URL" stands for "uniform resource locator," a combination of letters and numbers that comprise the digital "address" of a website.

[2] The technical details of how the FBI accomplishes this are mostly unimportant for the purposes of this appeal. Anytime you click on a website's content (e.g., a link, an image, a page), the website's host computer transmits data to your computer, allowing you to view the content that you requested. Ordinarily, this act is harmless, since most website owners are careful to give the user *only* what they requested. However, hackers and criminals sometimes embed secret "viruses" or "malware" in website content. If a user clicks on website content containing these nefarious programs, they are transmitted to the user's computer along with the requested content. Viruses can be programmed to do a broad range of things, from simply shutting down the user's machine to stealing information.

What the FBI did here is obtain authorization to place a "benevolent virus" on the target website, which installs itself on the user's machine when he or she clicks on any website content. The virus, instead of wreaking havoc, obediently transmits only the information permitted by the warrant. In this case, the warrant only permitted the virus to transmit (a) information identifying the physical location of the user's machine, and (b) information

"fingerprint" to the user's "pseudonym," and track what the person has viewed on the website. Police can also use a computer's IP address to discern its physical location through publicly available databases and routine subpoenas to companies like AT&T and Comcast. Thus, armed with the user's digital fingerprint, police can show a judge (a) what a user has viewed, and (b) where the user's computer is located in the real world.

B

This case began when the FBI obtained access to the physical computer running Playpen's website. The warrant permitting the FBI to use a bug is the "NIT warrant" in the record here.[3] Tagg does not really dispute that Playpen contained a significant amount of child pornography; neither does the government deny that Playpen also contained legal child erotica. After seizing Playpen's computers, the FBI kept the website running to try and catch some of its patrons. However, to identify Playpen's users, the FBI had to place a digital bug in the fabric of the website. Because this act counts as a Fourth Amendment "search" of the user's home computer—the bug creates a digital fingerprint that can identify the user—the FBI needed to obtain a warrant before embedding it. *United States v. Horton*, 863 F.3d 1041, 1046–47 (8th Cir. 2017), *cert. pet. filed in* No. 17-6910 (Nov. 21, 2017).

After collecting identifying data on the individual users of the website, the FBI and its local task-force affiliates sought separate, individual warrants for the homes of the identified users ("Residential Warrants"). To support these warrants, officers explained to federal magistrate judges how they cross-referenced the user's digital fingerprint with their pseudonym and IP address to connect three data points: (a) the user's identity, (b) the items the user had viewed on the website, and (c) the physical location and address of the user's computer.

---

distinguishing the user's machine from other computers at the same physical address. When a website is operating on the Tor network, this appears to be the only practical way for law enforcement to identify a website's users and gather necessary evidence. *See generally United States v. Workman*, 863 F.3d 1313, 1315–17 (10th Cir. 2017) (describing the technique), *cert. pet. filed in* No. 17-7042 (Oct. 3, 2017).

[3]These warrants have been the subject of much litigation, and their validity is still an open question. *United States v. Kahler*, 236 F. Supp. 3d 1009, 1017–18 (E.D. Mich. 2017) (collecting cases). The district judge below did not address the NIT warrant. Since the NIT warrant is not the subject of this appeal, we express no opinion on its validity today, and our opinion should not be construed to favor (or disfavor) these warrants as a matter of law. We cite its contents here merely for their value as background facts.

The affidavit supporting the Residential Warrant outlined Tagg's browsing history, which neither party disputes. The Residential Warrant therefore contained the following pieces of data. (1). Tagg spent around five hours logged into Playpen's website under the pseudonym "derpderk." (2). Tagg opened the website's "index" and browsed them for topics of interest to him. (3). He clicked on the "Pre-Teen Videos" entry in the index. That link took him to a separate part of the index where he could browse "Pre-teen Videos" in more detail. (4). After browsing that topic, Tagg viewed a collection of pages under the heading "Girls HC"—which, in the pornography world, means explicit, penetrative sexual acts. (5). Tagg then accessed the message board "video collection clow85."[4] (6). On other occasions, Tagg accessed pages titled, "Drug(g)ed sleeping girl 10yo fuck—", "girl Toy3-8y&man", and "PTHC[5] Anal dildo." The affidavit did not, however, state whether Tagg actually viewed or downloaded any illegal files.

The magistrate judge approved the Residential Warrant. The warrant indicated that officers had established probable cause that Tagg violated 18 U.S.C. § 2252A(a)(5) (access of a website with intent to view child pornography) and that evidence of the crime would be found at Tagg's residence. After searching Tagg's home, police found over 20,000 files of child pornography on his personal computers.

C

Tagg was charged with one count of receiving child pornography and one count of possessing the same. 18 U.S.C. § 2252A(a)(2), (a)(5)(B). Tagg moved to suppress all the evidence seized by the government, claiming that both the NIT Warrant and his individual Residential Warrant violated the Fourth Amendment. As noted above, the district court only addressed the Residential Warrant.

After a hearing, the district court held that the Residential Warrant was invalid. Specifically, the court held that police could not establish probable cause to search Tagg's home

[4]Although the parties do not indicate what "clow85" means, it appears to be the pseudonym of another user. Thus, "video collection clow85" is likely a collection of videos uploaded by the user clow85.

[5]The information in the affidavit indicates that "PTHC" is probably an acronym for "Pre-Teen Hard-Core."

for child pornography unless the supporting materials established that he actually clicked on or viewed an online file containing child pornography. Moreover, the court suppressed the evidence, reasoning that the good-faith exception did not apply because police acted recklessly and because no reasonable officer could have relied on the warrant. After its motion for reconsideration was denied, the government timely appealed. We have jurisdiction under 18 U.S.C. § 3731.

II

The district judge found that the Residential Warrant lacked probable cause. This was incorrect, particularly considering the Supreme Court's recent instructions in *District of Columbia v. Wesby*, 583 U.S. ___, 138 S. Ct. 577, 584–89 (2018) (examining probable cause "to arrest . . . partygoers for unlawful entry" in a civil action under 42 U.S.C. § 1983).

A

The Fourth Amendment prohibits judges from issuing search warrants unless the requesting officer demonstrates probable cause. U.S. Const. amend. IV. "A police officer has probable cause to conduct a search when the facts available to [the officer] would warrant a person of reasonable caution in the belief that contraband or evidence of a crime is present." *Florida v. Harris*, 568 U.S. 237, 243 (2013) (alterations and internal quotation marks omitted). A Supreme Court opinion, fresh off the press, has reminded the courts that "probable cause deals with probabilities and depends on the totality of the circumstances." *Wesby*, 138 S. Ct. at 586 (internal quotation marks omitted). Therefore, "[p]robable cause is not a high bar" and "is a fluid concept that is not readily, or even usefully, reduced to a neat set of legal rules." *Id.* (internal quotation marks omitted).

1

Probable cause "requires only a probability or substantial chance of criminal activity, not an actual showing of such activity." *Id.* (citation omitted). In determining probability, officers and magistrates may rely on "common-sense conclusions about human behavior." *Id.* at 587 (citation omitted); *see also United States v. Allen*, 211 F.3d 970, 975 (6th Cir. 2000) (en banc)

("Affidavits are not required to use magic words, nor does what is obvious in context need to be spelled out . . . ."). Moreover, judges are not permitted to engage in "an excessively technical dissection" of the record when determining probable cause. *Wesby*, 138 S. Ct. at 588 (internal quotation marks omitted) (reversing the Court of Appeals for examining a case this way). Facts must be considered *together*, not apart, since "the whole is often greater than the sum of its parts." *Id.* Finally—and most importantly for the purposes of this case—probable cause "does not require officers to rule out a suspect's innocent explanation for suspicious facts." *Id.* Instead, "the relevant inquiry is not whether particular conduct is 'innocent' or 'guilty,' but the degree of suspicion that attaches to particular types of noncriminal acts." *Id.* (quoting *Illinois v. Gates*, 462 U.S. 213, 244 n.13 (1983)).

Further, the court reviewing a warrant does not write on a blank slate. A judicial officer who issues a warrant "should be paid great deference." *Gates*, 462 U.S. at 236 (internal quotation marks omitted). The reviewing court is not permitted to attempt a de novo review of probable cause; the issuing judge's decision should be left undisturbed if there was a "substantial basis" for the probable-cause finding. *Id.* at 238–39; *United States v. King*, 227 F.3d 732, 739 (6th Cir. 2000). In service of this standard, an "affidavit is judged on the adequacy of what it does contain, not on what it lacks, or on what a critic might say should have been added." *Allen*, 211 F.3d at 975. An appellate court examines the reviewing judge's logic using a de novo standard. *United States v. Washington*, 380 F.3d 236, 240 (6th Cir. 2004).

2

We have been over this ground before in child-pornography cases. The unique challenges of child-pornography crimes demand a practical approach to the probable-cause question. *See United States v. Frechette*, 583 F.3d 374, 378 (6th Cir. 2009). We have repeatedly held that visiting or subscribing to a website containing child pornography creates a reasonable inference that the user has stored child pornography on their computer. *United States v. Wagers*, 452 F.3d 534, 538–40 (6th Cir. 2006); *Frechette*, 583 F.3d at 379; *United States v. Kinison*, 710 F.3d 678, 683–84 (6th Cir. 2013); *United States v. Elbe*, 774 F.3d 885, 889 (6th Cir. 2014) (discussing file exchanges on a peer-to-peer website). The fact that the website contains both legal and illegal material, while relevant, does not automatically negate probable cause. *Wagers*,

452 F.3d at 538–39. Indeed, we expressly rejected such an inflexible rule in *Wagers*, recognizing that a fact-intensive approach to probable cause was sufficient to deter overzealous law enforcement and prevent unwarranted invasions of privacy. *Id.* at 541–43.

We sustained this commitment to fact-based adjudication in *Frechette*. In that case, we held that a one-month, paid subscription to a website containing child pornography justified a reasonable officer in concluding that the user might have stored child pornography on his computer. *Frechette*, 583 F.3d at 380–81. Although the pattern of conduct alleged in the affidavit was less pervasive than in previous cases, we reasoned, "if someone spends $80 for something, it is highly likely that the person will use it—whether it is a tie, a video game, or a subscription to a pornographic web site." *Id.* at 380. Thus, it was "not likely" that the defendant "was innocently surfing the internet and accidentally paid $79.95 for a subscription" to a porn site. *Id.* at 381. Therefore, it was reasonable to think that the website's images may have ended up on the suspect's computer at some point, even though the warrant did not allege anything besides the subscription. *Id.* Like in *Wagers*, the panel rejected the defendant's bright-line rule, reasoning instead that fact-based examinations are enough.

3

We have also addressed the Fourth Amendment's nexus requirement as applied to the digital age. Probable cause to believe a *person* committed a crime does not justify a search of his or her residence absent some independent evidence linking the residence to the crime. *See United States v. Savoca*, 761 F.2d 292, 297 (6th Cir. 1985). However, we have held that a nexus exists when law enforcement connects the IP address used to access a website to the physical location identified by the warrant. *Elbe*, 774 F.3d at 890; *Kinison*, 710 F.3d at 683–84. Pointing to our "prior observations" that child pornography is typically possessed in the secrecy of the home, the *Kinison* panel reasoned that a search of the home was a perfectly logical next step for officers who have only circumstantial evidence of where the crime was committed and no "inside scoop" on which they could rely. 710 F.3d at 683–84.

B

The district court erred in holding that the warrant was not supported by probable cause. For that reason, it should have denied the motion to suppress.

The warrant was based on 18 U.S.C. § 2252A. That statute punishes any person who "knowingly accesses with intent to view, any . . . computer disk, or any other material that contains an image of child pornography." 18 U.S.C. § 2252A(a)(5)(B). It is elementary that an applicant for a search warrant need not allege facts establishing that a crime occurred. *Wesby* makes that perfectly clear. 138 S. Ct. at 586. Instead, the magistrate must ask whether the facts in the affidavit justified an officer of reasonable caution in suspecting that Tagg had accessed Playpen with the intent to view child pornography, and that evidence of that crime would be found on his home computer. That standard is unquestionably met here.

1

Tagg admits that he accessed the website. And the warrant application contained plenty of facts suggesting that he intended to view child pornography when he did so. First and foremost, it is unlikely that Tagg stumbled upon Playpen by accident. To access the site, he had to obtain the URL from someone "on the inside" who could provide the exact sequence of numbers and letters to enter into his browser. This creates an inference that Tagg deliberately accessed Playpen. Second, Tagg spent over five hours on the site, clicking on over 160 hyperlinks that were blatant advertisements for child pornography. *See, e.g.*, R. 29-1, Residential Warrant, PID 445, 451–52; *id.* at 446 ("Pre-teen Videos," "Girls [Hard-Core]"); *id.* at 452 ("Drug(g)ed sleeping girl 10yo fuck—"); *id.* ("Girl Toy3-8y&man"); *id.* ("[Pre-Teen Hard-Core] Anal dildo"). Indeed, when viewed alongside the other facts in the affidavit, such conduct makes it even more likely that Tagg intended to view child pornography when he accessed Playpen.

Further, the applicable criminal statute does not require a showing that Tagg actually viewed illegal content on the site. The access-with-intent offense is complete the moment that the elements of access and intent coincide. 18 U.S.C. § 2252A(a)(5)(B). Thus, even if the person never viewed illegal child pornography, knowingly accessing a child-pornography

website with the intent to view illegal materials is itself a criminal act. It follows from this language that probable cause to search Tagg's house would exist even if he was "curiosity shopping" for child porn on Playpen but never actually viewed an illegal image. *Id.* This is the most natural reading of the statute. Congress unambiguously set out to punish anyone who "knowingly possesses, *or* knowingly accesses with intent to view, any . . . computer disk . . . or other material . . . that contains an image of child pornography." *Id.* (emphasis added). Grammatically, the word "accesses" (the *actus reus* of the crime) is directed towards the repository containing child pornography, not the child pornography itself.

The person who completes the circle and views the image has, instead, committed the *actus reus* of possession. *See, e.g.*, *United States v. Ramos*, 685 F.3d 120, 130–32 (2d Cir. 2012) (holding that merely viewing child pornography in a web browser is sufficient to trigger "possession" liability under § 2252A(a)(5)). We agree with the Second Circuit that Congress intended the "possessing" *actus reus* to apply to someone who "intentionally searched for images of child pornography, found them, and knowingly accepted them onto his computer," even if that acceptance was merely temporary. *Id.* at 132. The logical conclusion of this rule is that "access-with-intent" liability is triggered when a person "intentionally searche[s] for images of child pornography, f[inds] them," but then stops short of viewing the images themselves. *See id.*; *Nat'l Ass'n of Mfrs. v. U.S. Dep't of Def.*, 138 S. Ct. 617, 632 (2018) (reversing a panel of this Court and reaffirming that we are "obliged to give effect, if possible, to every word Congress used" in a statute) (internal quotation marks omitted).

This approach mirrors the long-standing doctrine of attempt, which imposes liability on anyone who intends to do an illegal act and takes a substantial step toward that goal. *United States v. Resendiz-Ponce*, 549 U.S. 102, 106–08 (2007). Even if it seems harsh, Congress has unambiguously declared that the act of accessing a website containing child porn—when done with criminal intent—is a sufficiently "substantial" step to warrant criminal sanctions. *See id.*; 18 U.S.C. § 2252A(a)(5). And when Congress speaks clearly, we may not frustrate its intent via lenient interpretation. *Cf. Shaw v. United States*, 137 S. Ct. 462, 469 (2016).

2

The Eighth Circuit has implicitly taken this broad view of the criminal liability provision of the statute in two recent cases. *United States v. DeFoggi*, 839 F.3d 701, 711–12 (8th Cir. 2016); *United States v. Huyck*, 849 F.3d 432, 442–43 (8th Cir. 2017). In *Huyck*, the defendant was convicted of separate instances of possession and access with intent to view child pornography. *Huyck*, 849 F.3d at 442. In rejecting a sufficiency challenge to the access-with-intent charge, the Eighth Circuit pointed to three facts which carried the government's burden: (a) circumstantial evidence that Huyck's computers ran the same browser and operating system detected by the NIT surveillance system; (b) a text file on Huyck's computer containing instructions on how to use Tor and links to several "secret" child-pornography websites; and (c) Huyck's admission that he had used Tor in the past. *Id.* The panel did not discuss whether or not the government offered proof that Huyck had ever accessed images from that website, instead reasoning that the conviction should stand because the evidence "demonstrat[ed] his knowledge and intent to use the Tor network to receive and access child pornography." *Id.*

DeFoggi is equally stern. In that case, the defendant was a member of "PedoBook," a child-pornography site on the Tor network. While on the site, he engaged in "copious amounts of discussion concerning the exchange of child pornography with other users." *DeFoggi*, 839 F.3d at 711–12 (citation omitted). The defendant sought to void his conviction, reasoning that his chats were "mere fantasy" and did not indicate an intent to view child pornography. *Id.* at 712. The court was not persuaded. Pointing out that he had "asked other members of PedoBook where he could find certain videos and whether they had or could produce images for him," the court reasoned that the jury could have reasonably concluded that he intended to view child pornography. *Id.* Although police caught the defendant in the act of downloading a video when they executed a warrant at his residence, this fact did not seem particularly important to the panel, as it would have been if it was an essential part of the proofs. *Id.* *DeFoggi* and *Huyck* are out-of-circuit cases addressing the sufficiency of the evidence, not probable cause, but they nevertheless provide some insight into what the access-with-intent clause of the statute prohibits.

We emphasize that the scienter requirement of this statute imposes an unforgiving standard on the government. Indeed, the government conceded at oral argument that—in the

absence of proof that a person actually viewed or possessed any child pornography—it may be difficult to prove intent beyond a reasonable doubt at trial. This is as it should be. Child pornography receives no protection from the First Amendment, but the Supreme Court has made it clear that a strict *mens rea* is a key factor in policing overbreadth and ensuring that "unwitting" users are not punished for protected speech. *See United States v. Williams*, 553 U.S. 285, 288–89 (2008); *United States v. Woods*, 684 F.3d 1045, 1060 (11th Cir. 2012); *United States v. Brune*, 767 F.3d 1009, 1020–21 (10th Cir. 2014). But in the probable-cause context, we are content that on the facts of this case, a reasonable officer could infer that Tagg formed the required intent at some point during the five hours he spent browsing Playpen.

Tagg insists that the affidavit "did not offer facts to show [he] acted with specific 'intent to access'" child pornography. This, again, conflates probable cause with proof; the affidavit need not "show" that Tagg had unlawful intent—it only needed to allege facts that create a reasonable probability that Tagg had an unlawful motive. *See Wesby*, 138 S. Ct. at 586 (stating that probable cause does not require "an actual showing" of illegal conduct) (internal quotation marks omitted). Tagg tries to weaken this inference by pointing out that the site also distributed legal child erotica. He seizes on this fact to argue that he intended to view child erotica, not illegal child pornography, and therefore that the warrant could not establish probable cause. The Supreme Court disagrees. *Wesby* makes clear that the ultimate plausibility of an innocent explanation cannot be used to snuff out the objectively suspicious inference that can be drawn from the facts presented to a magistrate. *See id.* at 588. Tagg may or may not be guilty of a crime, and we reiterate that this would be a different case if the government sought to sustain a conviction based solely on the statements in this affidavit. But police need not "rule out a suspect's innocent explanation for suspicious facts" in order to establish probable cause, and Tagg may not litigate the issue of guilt or innocence on a motion to suppress. *See id.*

In sum, the plain language of the statute penalizes anyone who knowingly accesses a website that contains child pornography *and* who intends to view that illegal content, even if he never actually does so. It follows that a warrant may issue against someone like Tagg when law enforcement shows that the suspect (a) accessed a website containing actual child pornography,

and (b) browsed the site for an extended period of time while clicking on links that were blatant advertisements for child pornography.

3

Tagg also challenges the nexus element of the search. He insists that the mere fact that he used a computer to commit a crime does not automatically justify a search of his residence. This, of course, is correct. *See generally Peffer v. Stephens*, 880 F.3d 256, 266–74 (6th Cir. 2018); *Savoca*, 761 F.2d at 297. But Tagg ignores the fact that police linked the IP address he used to access Playpen to the residence listed on the warrant, and even observed him entering and exiting the premises. Our precedent holds that this is enough to establish a nexus. *Elbe*, 774 F.3d at 890; *Kinison*, 710 F.3d at 683–84; *see also United States v. Lapsins*, 570 F.3d 758, 766–67 (6th Cir. 2009).

III

Tagg cites several out-of-circuit cases to persuade us to affirm the district court's suppression order. *United States v. Raymonda*, 780 F.3d 105 (2d Cir. 2015); *United States v. Falso*, 544 F.3d 110 (2d Cir. 2008); *United States v. Edwards*, 813 F.3d 953 (10th Cir. 2015). He misapprehends the helpfulness of these cases, however, as they actually support the government's position. In fact, the Second Circuit extended our decision in *Frechette* to an unpaid registration for a pornographic website, reasoning that the mere act of signing up for a "members-only" child-pornography site was enough to establish probable cause to search the defendant's home. *Raymonda*, 780 F.3d at 115–16 (discussing *United States v. Martin*, 426 F.3d 68 (2d Cir. 2005)).

Raymonda then contrasted *Martin* with *Falso*, the second case on which Tagg relies. In *Falso*, the warrant merely alleged that the defendant tried (possibly unsuccessfully) to access a website containing child pornography. 544 F.3d at 121. The *Falso* panel held that probable cause could not exist under those circumstances unless the warrant contained "specific allegations" that the defendant actually viewed child pornography. *Id.* In contrast, Tagg was a registered member of Playpen and successfully accessed the site for over five hours.

Thus, the Second Circuit's cases are even less favorable to Tagg than our own. Indeed, *Raymonda* endorsed a legal conclusion not yet present in our case law—that "*the fact of membership* to a child-pornography website," paid or unpaid, creates probable cause to search the member's home computer. *Raymonda*, 780 F.3d at 116 (quoting *Falso*, 544 F.3d at 121) (emphasis added by the *Raymonda* panel). Tagg was a member of Playpen in the sense that *Martin* used that word. *Raymonda* also emphasized that this fact was crucial in distinguishing between *Martin* and *Falso*, since the *Falso* defendant had not subscribed to a members-only website. *Raymonda*, 780 F.3d at 115–16.

Raymonda's facts are also distinguishable. The warrant in *Raymonda* only alleged that on one afternoon, nine months ago, the defendant opened one or two pages of a website containing child-pornography files. *Id.* at 116–17. The Second Circuit was simply not persuaded that this was sufficient to support probable cause for a residential search. In contrast, Tagg accessed Playpen for five hours over thirty days and viewed hundreds of pages containing child-pornography files. The facts here—critical in probable-cause determinations—simply do not compare.

Finally, Tagg stretches the Tenth Circuit's decision in *Edwards* to mean more than what it says. In *Edwards*, the affidavit only alleged that the defendant possessed and shared child erotica, not child pornography. *Edwards*, 813 F.3d at 960–61. Importantly, the warrant in that case never alleged that the suspect possessed, searched for, browsed, or made any effort to engage with actual child pornography. *Id.* at 962–63. In rejecting the government's arguments, the Tenth Circuit held that mere interest in child erotica or sexual attraction to children was insufficient, standing alone, to cause an officer of reasonable caution to suspect someone of a crime. *Id.* at 964–65.

We have rejected similar attempts by the government to use evidence of child molestation to support warrants for child pornography. *E.g.*, *United States v. Hodson*, 543 F.3d 286, 292–94 (6th Cir. 2008); *see also United States v. Doyle*, 650 F.3d 460, 472 (4th Cir. 2011) ("The bulk of the information supplied in the affidavit concerned allegations of sexual assault. But evidence of child molestation alone does not support probable cause to search for child pornography." (citing *Hodson*, 543 F.3d at 292)). However, the logic of *Edwards* and *Hodson*

does not apply to defendants, like Tagg, who interact with the child-pornography components of a website. In those cases, *Frechette* and *Wagers* must control. *Frechette*, 583 F.3d at 380–81; *Wagers*, 452 F.3d at 538–40.

IV

The warrant below was supported by probable cause; it was error to suppress the evidence seized under its authority. Therefore, the district court's order granting the motion to suppress is **REVERSED**, and the case is **REMANDED** for proceedings not inconsistent with this opinion.

CONCURRENCE

JANE B. STRANCH, Circuit Judge, concurring. I concur in today's decision because, taken together, Tagg's registration of a Playpen account, which was necessary to access the portions of the website that contained child pornography, his sustained activity on Playpen, and his deliberate navigation to multiple forums clearly devoted to child pornography created probable cause to issue the Residential Warrant. I write separately only to note that *United States v. Ramos*, 685 F.3d 120 (2d Cir. 2012), is an out-of-circuit case concerning a later stage of criminal prosecution and a different crime. *Ramos* is therefore immaterial to the probable cause determination in Tagg's case. *See id.* at 131 (holding that "that the evidence was sufficient to prove [at trial] that Ramos was guilty of knowingly receiving and possessing child pornography"). Although we have no cause to apply *Ramos*, I otherwise agree that the constellation of facts contained in the affidavit call for reversing the district court's suppression decision.