13-4899-cr
United States v. Raymonda

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

August Term, 2014

(Argued: November 3, 2014 Decided: March 2, 2015)

Docket No. 13-4899-cr

UNITED STATES OF AMERICA,

Appellant,

— v. —

JAMES RAYMONDA,

Defendant-Appellee.

B e f o r e:

WALKER, LYNCH, and CHIN, *Circuit Judges*.

The government appeals from an order of the district court suppressing evidence of child pornography obtained at James Raymonda's home on the grounds that the search warrant, issued on the basis of a single incident of access to online child pornography more than nine months earlier, was not supported by probable cause. The government argues that the evidence should not be suppressed, because the known propensity of child pornography enthusiasts to hoard pornographic images precludes a finding of staleness and because the executing officers were entitled to rely in good faith on the search warrant. We hold that evidence of access to child pornography on a single occasion, absent any indicia of the suspect's deliberate intention to access those images, does not support an inference that the suspect is a hoarder of child pornography sufficient to create probable cause to believe that child pornography will be found at the suspect's home nine months later. Nevertheless, we further hold that suppression of the evidence was not required because the agents executing the search relied in good faith on a duly issued warrant.

REVERSED.

Denny Chin, *Circuit Judge*, filed a separate opinion, concurring in part and dissenting in part.

MONICA J. RICHARDS, Assistant United States Attorney, *for* William J. Hochul, Jr., United States Attorney for the Western District of New York, Buffalo, New York.

MARYBETH COVERT, Assistant Federal Defender, Federal Public Defender's Office, Western District of New York, Buffalo, New York, *for Defendant-Appellee* James Raymonda.

GERARD E. LYNCH, *Circuit Judge*:

More than nine months after someone using defendant-appellee James Raymonda's IP address accessed thumbnail images of child pornography on the Internet, government agents obtained a search warrant for his home and discovered over one thousand files of child pornography. The United States District Court for the Western District of New York (William M. Skretny, *Chief Judge*) granted Raymonda's motion to suppress, finding that the government's evidence that Raymonda had accessed child pornography on a single occasion nine months earlier was too stale to establish probable cause that he would still possess illicit images at the time of the search. The United States appeals that decision, arguing that the recognized propensity of persons interested in child

pornography to collect and hoard such images supports an inference that Raymonda would still possess child pornography when the warrant was sought. Alternatively, the government argues that, even if probable cause was lacking, the evidence should not be suppressed because the agents who executed the search relied in good faith on a warrant duly issued by a judicial officer.

We agree with the district court that a single incident of access to thumbnail images of child pornography, absent any other circumstances suggesting that the suspect accessed those images deliberately or has a continuing interest in child pornography, fails to establish probable cause that the suspect will possess illicit images many months later. However, because the agents in this case relied in good faith on a magistrate judge's independent determination of probable cause, we reverse the district court's order granting Raymonda's suppression motion.

BACKGROUND

I. The Investigation

On January 13, 2011, U.S. Immigration and Customs Enforcement ("ICE") Special Agent Eric Sajo of the San Diego Cyber Crimes Unit discovered a link on the website www.motherless.com. Posted under a discussion thread dedicated

to discussing administrative website content, such as "bugs, feature requests, complaints, or other site related materials," the link redirected Agent Sajo to the website "www.coolib.org." That site featured numerous thumbnail links to images of child pornography, spread across several pages hosting up to approximately thirty thumbnails each.

After Agent Sajo obtained a search warrant for the website content of www.coolib.org, the site's host company provided records that included 861 images of child pornography, as well as access log information for each image posted to the site. The host company also produced Internet Protocol ("IP") logs for individual users who had visited the website, tracking GET requests automatically generated when a user's web browser downloaded the thumbnails on each web page.[1] Organized by individual user, the IP logs indicated which specific files the user's browser had accessed or attempted to access and when the access or attempted access had occurred. Due to the host company's server configurations, the only IP logs available were those for January 16, 2011.

The IP logs revealed that, on January 16, 2011, a user with a particular IP

[1] A GET request is a message sent from an HTTP client, such as a web browser, to a server asking for the content located at a particular URL.

address accessed 76 images from www.coolib.org, the majority of which were thumbnail images of child pornography. Although the IP logs were not organized chronologically, the time stamps on the GET requests suggested that all 76 images were accessed over a period of seventeen seconds. The log showed no user requests for any full-sized versions of the thumbnail images.

On July 13, 2011, Time Warner Cable identified the Internet subscriber associated with that IP address on January 16, 2011 as James Raymonda of Buffalo, New York. The United States Postal Service subsequently confirmed that Raymonda currently received mail at the address associated with that account.

II. The Warrant

Based on the foregoing information, on October 27, 2011, Special Agent Adam J. Ouzer of the Homeland Security Investigations division ("HSI") of the Department of Homeland Security applied for a warrant to search the property at Raymonda's address for violations of 18 U.S.C. §§ 2252 and 2252A, which prohibit the distribution, possession, or receipt of child pornography.

In support of the application, Agent Ouzer included an affidavit disclosing the details of Agent Sajo's investigation, including Agent Sajo's discovery of

www.coolib.org through a link on www.motherless.com, his acquisition of user logs for the IP address in question, and his confirmation that this IP address was associated with Raymonda. Discussing the content of the IP logs, Agent Ouzer stated that "76 images, the majority of which were images of child pornography, . . . were accessed by the user of [the] IP address." While conceding that these logs provided "no record that the user accessed an enlarged (full size) image," Agent Ouzer concluded that they nevertheless "show more than one incidence of access of thumbnail images by the user." He also stated that the logs "identified that the user of [the] IP address . . . successfully viewed suspect child pornography images contained in Directory 55," and that "the frequency of successful (GET) requests for the suspect images" contained in the log "provide evidence that the user intended to view the content." Agent Ouzer did not append the full IP log to his warrant application, nor did he state that the time stamps on the log covered a span of seventeen seconds.

In addition to his account of the investigation, Agent Ouzer's affidavit included numerous boilerplate paragraphs describing the online trade in child pornography and the logistics of recovering digital data from computer hard drives. Agent Ouzer testified that the abundance of information-sharing

technologies on the Internet have made computers "a preferred method of distribution and receipt of child pornographic materials," and that computers' capacity "to store images in digital form makes [them] an ideal repository of child pornography." Fortunately for investigators, because electronic data stays in a computer's residual memory long after deletion, forensic specialists can recover even ostensibly deleted pornographic files "months or even years after they have been downloaded onto a hard drive . . . or viewed via the Internet." Even Internet files that are "automatically downloaded into a temporary Internet directory . . . are only overwritten as they are replaced with more recently viewed" files.

Finally, Agent Ouzer stated that his experience investigating child pornography cases had revealed certain common propensities among persons interested in child pornography. "Individuals who have a sexual interest in children" commonly hoard images of child pornography, "retain[ing] pictures, films, photographs, negatives, . . . and videotapes for many years." Even digital images, seemingly replaceable, "are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly." Agent Ouzer concluded that the

"person(s) residing at the SUBJECT PREMISES exhibits the common characteristics described above of someone involved in the distribution, receipt, and possession of child pornography."

Based on Agent Ouzer's application, a magistrate judge issued a search warrant for Raymonda's address. Agent Ouzer and several other HSI agents executed the warrant on November 8, 2011. While several agents searched the house, Agent Ouzer and a colleague asked Raymonda to speak with them outside. The agents told Raymonda about the nature of the warrant, but advised that he was not under arrest and was free to leave. Raymonda nevertheless agreed to speak with them and, in the ensuing conversation, admitted to viewing child pornography online.

Inside the home, HSI agents seized two laptops, a tower computer, and an external hard drive. These items were later found to contain over 1,000 images of child pornography.

III. Indictment and Motion to Suppress

On December 21, 2011, Raymonda was indicted in the Western District of New York on one charge of knowingly receiving child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A) and four charges of knowingly possessing child

pornography in violation of 18 U.S.C. § 2252A(a)(5)(B).

On March 19, 2012, Raymonda filed a motion to suppress all evidence discovered at his home on November 8, 2011, including his statements to Agent Ouzer, arguing that the search warrant was issued without probable cause and that Agent Ouzer had not relied on that warrant in good faith. Specifically, Raymonda argued that Agent Ouzer's evidence that a user with his IP address allegedly accessed images of child pornography in January 2011 was too stale to suggest that pornographic images would still be found in his home at the time of the search, and that Agent Ouzer's involvement in United States v. Coon, No. 10-CR-110A, 2011 WL 1871165, (W.D.N.Y. May 16, 2011), an earlier case in which one-year-old evidence of possession had been found too stale to create probable cause, should have alerted him to the deficiency.

In support of his motion, Raymonda introduced the expert testimony of Gerald R. Grant, a forensic investigator with the Federal Public Defender's office. Grant testified that GET requests for images contained in an IP log do not signal that a user intentionally opened or clicked on individual links, but rather occur automatically whenever a browser opens a web page: "If you're on the internet browsing, and you click on a web page, and that web page comes up on your

screen, that web page is a series of get commands . . . ." Accordingly, the IP logs obtained for www.coolib.org did not disclose whether the user with Raymonda's IP address had saved or even viewed all of the images that his browser had accessed, and indeed would have looked exactly the same even if he "simply close[d]" the site immediately after clicking on it. Grant clarified that images automatically downloaded by a user's web browser are not saved to the user's hard drive, but only to a temporary Internet cache where they typically remain "two days to a month" before being overwritten. Finally, he noted that all images accessed by the user were downloaded within seventeen seconds, a time span consistent with a web browser loading images on a single page at slightly different speeds.

Raymonda also introduced the testimony of Agent Ouzer's direct supervisor in Coon and the prosecutor who tried the case. While neither witness had a "specific recollection" of discussing the staleness challenge with Agent Ouzer, both testified that their general practice was to inform the agent involved in their cases of any challenges to the validity of a warrant.

Testifying at the hearing, Agent Ouzer reiterated his understanding that the IP logs obtained for Raymonda's IP address suggested that the user had in

fact intentionally accessed child pornography, stating that each GET request signified that an individual had "clicked on the image" or "attempted to receive the larger image by clicking on the thumbnail." He also testified that any pornographic images viewed by Raymonda on www.coolib.org "would have been downloaded on [his] computer," though he admitted he did not know where precisely they would be saved. While acknowledging his involvement as the investigator in Coon, Agent Ouzer did not recall ever having learned that the judge in that case found the year-old evidence in his affidavit stale.

IV. District Court Orders

On April 5, 2013, Magistrate Judge Hugh B. Scott issued a Report and Recommendation urging the court to suppress all evidence obtained through the search warrant. Judge Scott found that, contrary to the suggestions in Agent Ouzer's affidavit, the IP logs did not disclose that the user with Raymonda's IP address had engaged in "more than one incidence of access" so as to view 76 separate images, but were consistent with images loading automatically upon a single visit to the offending website. He noted that the affidavit had contained no corroborative evidence of Raymonda's general interest in child pornography, nor any evidence that Raymonda had saved the illicit images to his hard drive.

Crediting Grant's testimony that temporary Internet files are typically deleted within a month and lacking any evidence that Raymonda "fits the profile of an individual who hoards . . . child pornography," Judge Scott found no probable cause to believe that pornographic images would still have been on Raymonda's computer, or otherwise in his possession, at the time of the warrant application.

Judge Scott also concluded that Agent Ouzer was not entitled to the good faith exception to the exclusionary rule. As factual matter, he found that Agent Ouzer must have known about the suppression order in Coon, which should have alerted him to the staleness of the nine-month-old IP logs. Furthermore, Judge Scott noted that Agent Ouzer's affidavit contained "misleading statements that significantly exaggerated" the import of his evidence, including his suggestions that the IP logs showed "more than one incidence of access," that Raymonda accessed 76 separate files, and that Raymonda was involved in the "distribution" of child pornography. While disclaiming any conclusion that Agent Ouzer had intentionally deceived the issuing magistrate, the judge nevertheless concluded that his affidavit was so "grossly negligent" so as to merit suppression.

On July 23, 2013, Chief Judge William M. Skretny of the United States

District Court for the Western District of New York adopted the Report and Recommendation in full. Chief Judge Skretny emphasized that although the "agents did not intentionally present misleading information . . . , their conduct did involve some degree of negligence" counseling against application of the good faith exception. He subsequently denied the government's motion for reconsideration, clarifying that his earlier order did not supplant Judge Scott's factual findings, but rather "accepted the Report and Recommendation – and the Magistrate Judge's findings concerning misleading statements and gross negligence – without modification."

DISCUSSION

On appeal from a district court's ruling on a motion to suppress, we review the court's factual findings for clear error. United States v. Smith, 9 F.3d 1007, 1011 (2d Cir. 1993). We review the court's legal determinations, including the existence of probable cause and the good faith of officers relying on a search warrant, de novo.[2] Id.

[2] The dissent's conclusion that the good faith exception to the exclusionary rule does not apply rests largely on its disagreement with this standard of review. See Dissent at 11-12. It is well established in this Circuit that we review a district court's determination of an officer's good faith reliance on an issued warrant de novo. See, e.g., United States v. Clark, 638 F.3d 89, 93 (2d Cir. 2011); United

The government presses two chief arguments on appeal. First, it argues that the nine-month gap between the IP logs and the warrant application did not render the evidence in Agent Ouzer's affidavit stale, because persons interested in child pornography are known to hoard digital files for extensive periods of time. Second, it argues that Agent Ouzer was entitled to the good faith exception because the suppression order in Coon did not establish a binding rule of law and because Agent Ouzer's alleged misstatements did not amount to gross negligence.

I. Probable Cause

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation." U.S. Const. amend. IV. Probable cause "is a fluid concept" turning "on the assessment of probabilities in particular factual contexts," and as such is not "readily, or even usefully, reduced to a neat set of legal rules." United States v. Falso, 544 F.3d 110, 117 (2d Cir. 2008), quoting Illinois v. Gates, 462 U.S. 213, 232 (1983). In evaluating probable cause in any given case, a judge must "make a practical, common-sense decision

---

States v. Irving, 452 F.3d 110, 125 (2d Cir. 2006); United States v. Gagnon, 373 F.3d 230, 235 (2d Cir. 2004).

whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." Id. (alterations in original), quoting Gates, 462 U.S. at 238. Due to this subjective standard, a reviewing court generally accords "substantial deference to the finding of an issuing judicial officer that probable cause exists," limiting our inquiry to whether the officer "had a substantial basis" for his determination. United States v. Wagner, 989 F.2d 69, 72 (2d Cir. 1993). Even applying this standard, however, we may conclude that a warrant is invalid where the magistrate's "probable-cause determination reflect[s] an improper analysis of the totality of circumstances." Falso, 544 F.3d at 117 (internal quotation marks omitted).

In particular, we may conclude that a warrant lacks probable cause where the evidence supporting it is not "sufficiently close in time to the issuance of the warrant" that "probable cause can be said to exist *as of the time of the search*" – that is, where the facts supporting criminal activity have grown stale by the time that the warrant issues. Wagner, 989 F.2d at 75 (emphasis added). The law recognizes "no bright-line rule for staleness," Walczyk v. Rio, 496 F.3d 139, 162 (2d Cir. 2007), which must instead be evaluated "on the basis of the facts of each

case," United States v. Martino, 664 F.2d 860, 867 (2d Cir. 1981). The two critical factors in determining staleness are the age of the facts alleged and the "nature of the conduct alleged to have violated the law." United States v. Ortiz, 143 F.3d 728, 732 (2d Cir. 1998) (internal quotation marks omitted). Where the affidavit "establishes a pattern of continuing criminal activity," such that "there is reason to believe that the cited activity was probably not a one-time occurrence," the passage of time between the last alleged event and the warrant application is less significant. Wagner, 989 F.2d at 75.

We have recognized that the determination of staleness in investigations involving child pornography is "unique." United States v. Irving, 452 F.3d 110, 125 (2d Cir. 2006). Because "it is well known that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes," evidence that such persons possessed child pornography in the past supports a reasonable inference that they retain those images – or have obtained new ones – in the present. Id. (internal quotation marks omitted); see also United States v. Vosburgh, 602 F.3d 512, 528 (3d Cir. 2010) ("[P]ersons with an interest in child pornography tend to hoard their materials and retain them for a long time."); United States v. Gourde, 440 F.3d 1065, 1072 (9th Cir. 2006)

("Collectors act like pack rats . . . [,] rarely, if ever, dispos[ing] of their sexually explicit materials.") (internal quotation marks omitted). Crucially, however, the value of that inference in any given case depends on the preliminary finding that the suspect is a person "interested in" images of child pornography. The "alleged 'proclivities' of collectors of child pornography," that is, "are only relevant if there is probable cause to believe that [a given defendant] *is* such a collector." United States v. Coreas, 419 F.3d 151, 156 (2d Cir. 2005) (emphasis added).

Federal courts including this one have historically inferred that a suspect is a "collector" of child pornography, likely to hoard illicit images, based on a number of factors. They have done so given a suspect's admission or other evidence identifying him as a "pedophile." See, e.g., Irving, 452 F.3d at 125 (finding no staleness where suspect "admitted he was a convicted pedophile," id. at 115); United States v. Harvey, 2 F.3d 1318, 1323 (3d Cir. 1993) (finding no staleness where affidavit "provided ample information that [suspect] was a pedophile"). They have done so in light of information that the suspect paid for access to child pornography. See, e.g., United States v. Frechette, 583 F.3d 374, 379 (6th Cir. 2009) (finding no staleness where suspect purchased $79.95 website

subscription); Gourde, 440 F.3d at 1072 (finding that suspect "fit the collector profile because he joined a paid subscription website dedicated to child pornography"); United States v. Payne, 519 F. Supp. 2d 466, 477-78 (D.N.J. 2007), aff'd, 394 F. App'x 891 (3d Cir. 2010) (finding no staleness where suspect purchased "paid subscription"). And they have done so where the suspect had an extended history of possessing or receiving pornographic images. See, e.g., United States v. Pappas, 592 F.3d 799, 802-03 (7th Cir. 2010) (finding no staleness where suspect received eleven pornographic mailings over two months); United States v. Allen, 625 F.3d 830, 842-43 (5th Cir. 2010) (finding no staleness where suspect had history of trading child pornography); United States v. Cox, 190 F. Supp. 2d 330, 334 (N.D.N.Y. 2002) (finding no staleness where suspect "received numerous images of child erotica and child pornography over an almost three-year period").

In certain circumstances, courts have even inferred that a suspect was a hoarder of child pornography on the basis of a single incident of possession or receipt. They have done so where, for example, the suspect's access to the pornographic images depended on a series of sufficiently complicated steps to suggest his willful intention to view the files. See, e.g., Vosburgh, 602 F.3d at 528

(finding no staleness where suspect could not have accessed images "with a simple click of the mouse," but had to enter decoded URL address and decrypt ensuing download, id. at 517); United States v. Hay, 231 F.3d 630, 634, 636 (9th Cir. 2000) (finding no staleness where suspect received 19 files within seven minutes through file transfer protocol). Or they have done so where the defendant, having accessed a single file of child pornography, subsequently redistributed that file to other users. See, e.g., United States v. Seiver, 692 F.3d 774, 775-77 (7th Cir. 2012) (finding no staleness where suspect downloaded single video and subsequently uploaded still images from video to Internet).

In all of these cases, the inference that the suspect was a collector of child pornography did not proceed merely from evidence of his access to child pornography at a single time in the past. Rather, it proceeded from circumstances suggesting that he had accessed those images willfully and deliberately, actively seeking them out to satisfy a preexisting predilection. Such circumstances tend to negate the possibility that a suspect's brush with child pornography was a purely negligent or inadvertent encounter, the residue of which was long ago expunged. They suggest that the suspect accessed those images because he was specifically interested in child pornography, and thus – as

is common among persons interested in child pornography – likely hoarded the images he found. As the Sixth Circuit has observed, "[i]t is not likely that . . . someone who was innocently surfing the internet . . . accidentally paid $79.95 for a subscription to [a child pornography] web site." Frechette, 583 F.3d at 381; see also United States v. Shields, 458 F.3d 269, 279 (3d Cir. 2006) ("[The possibility] that an individual . . . simply might have stumbled upon the sites . . . is remote given his registrations . . . and his subsequent failure to cancel his memberships.") (internal quotation marks and alteration omitted).

That insight is consistent with our own cases discussing child pornography. While we have never addressed the circumstances under which a suspect's online access to images of child pornography raises the inference that he will hoard those images so as to defeat a staleness challenge, we have on at least two occasions considered when a suspect's *recent* online activity creates probable cause to search his computer for child pornography. See Falso, 544 F.3d 110; United States v. Martin, 426 F.3d 68 (2d Cir. 2005).[3] In Martin, we upheld a warrant to search a suspect's computer for pornographic images on the grounds

[3] We also addressed that issue in Coreas, 419 F.3d at 156. Because Coreas ultimately deferred entirely to Martin in its analysis of probable cause, however, see id. at 159, it adds no precedential analysis on this point.

that he had recently joined an Internet group devoted to the distribution of child pornography, even absent evidence that he had actually accessed any illicit images through that site. 426 F.3d at 73. In doing so, we stressed that the suspect had voluntarily "joined . . . and never cancelled his membership" in a website built around facilitating access to child pornography. Id. at 75. Because it was "common sense that an individual who joins such a site would more than likely download and possess such material," the fact that Martin had deliberately registered an account with the group strongly suggested that he was actively interested in its materials and therefore sought out pornographic files. Id.; see also United States v. Froman, 355 F.3d 882, 890 (5th Cir. 2004) ("[T]he magistrate was entitled to conclude that the overriding reason someone would join [a child pornography] group was to permit him to receive and trade child pornography.").

By contrast, in Falso we held that the mere fact the defendant had apparently tried to access a non-membership website featuring images of child pornography, absent any evidence that he subsequently viewed those images, did not establish probable cause to search his computer. 544 F.3d at 121. Distinguishing Martin, we emphasized the significance of Martin's registration in

a members-only pornographic website to the finding of probable cause in that case. Id. Because "membership in the egroup reasonably implied use of the website," id., quoting Martin, 426 F.3d at 75, we stressed that "it [wa]s *the fact of membership* to a child-pornography website that largely supports the inference[ ] . . . that the defendant more likely than not used the website and downloaded images from it," id. (emphasis added). Absent similar circumstances suggesting that Falso had come upon the website for the *purpose* of finding child pornography, the mere fact that he visited or tried to visit a website that could have provided access to pornographic images did not create a fair probability that he subsequently obtained access to those images. Id. at 120. Probable cause to search the suspect's premises for possession, in short, depended not merely on his *opportunity* to possess child pornography at the time of the warrant application, but on his demonstrable interest in doing so.

In explaining its ultimate refusal to find probable cause, the panel in Falso went on to observe that there were "no specific allegation[s] that Falso accessed, viewed or downloaded child pornography." Id. at 121. But that observation does not compel a finding of probable cause in this case. To begin with, Agent Ouzer's affidavit contained no evidence that the suspect downloaded any images

of child pornography from www.coolib.org, suggesting instead that the IP user did not even click on any thumbnail links to access the full-sized files. Moreover, Falso was not a case involving stale evidence. In Falso, agents sought a warrant to search the suspect's computer based on entirely current information. In such a case, any evidence that the suspect had recently "accessed" child pornography would necessarily have supported an inference that some traces of illicit images, at the very least, could be recovered in his computer's temporary memory. Even lacking any independent indicia of the suspect's deliberate or "knowing" access to those images – necessary to establish criminal guilt at trial – such information would certainly support a "fair probability" that some relevant evidence of a crime would be found on the suspect's computer. See Gates, 462 U.S. at 238.

By contrast, to establish probable cause in this case, where the agents applied for a warrant on the basis of nine-month-old evidence, it was not enough simply to show that the suspect had at some point accessed thumbnails of child pornography. It was necessary to show that he accessed them in circumstances sufficiently deliberate or willful to suggest that he was an intentional "collector" of child pornography, likely to hoard those images – or acquire new ones – long after any automatic traces of that initial incident had cleared. No such

propensity-raising circumstances are present in the record. Agent Ouzer's affidavit alleged only that, on a single afternoon more than nine months earlier, a user with an IP address associated with Raymonda's home opened between one and three pages of a website housing thumbnail links to images of child pornography, but did not click on any thumbnails to view the full-sized files.[4] The affidavit contained no evidence suggesting that the user had deliberately sought to view those thumbnails or that he discovered www.coolib.org while searching for child pornography – especially considering that Agent Sajo himself only uncovered the website through an innocuous link on the message board of another site not explicitly associated with child pornography. Nor was there any evidence that the user subsequently saved the illicit thumbnails to his hard drive, or that he even saw all of the images, many of which may have downloaded in his browser outside immediate view. Far from suggesting a knowing and intentional search for child pornography, in short, the information in Agent Ouzer's affidavit was at least equally consistent with an innocent user

[4] Because Raymonda's motion to suppress challenges the warrant solely on the basis of staleness, rather than any material omissions in the affidavit, see Franks v. Delaware, 438 U.S. 154 (1978), our analysis of probable cause does not rely on the additional fact, found by the district court but not known to the magistrate judge who issued the warrant, that all images loaded within seventeen seconds.

inadvertently stumbling upon a child pornography website, being horrified at what he saw, and promptly closing the window.

Under those circumstances, absent any indicia that the suspect was a collector of child pornography likely to hoard pornographic files, we hold that a single incident of access does not create a fair probability that child pornography will still be found on a suspect's computer months after all temporary traces of that incident have likely cleared. We thus conclude that the warrant issued in this case was not supported by probable cause.

II. Good Faith

That the warrant was not supported by probable cause, however, does not necessarily mean that the evidence discovered by the agents at Raymonda's home must be suppressed.

The exclusion of evidence obtained in violation of the Fourth Amendment is a "prudential" remedy, crafted by the Supreme Court "to compel respect for the constitutional guaranty." Davis v. United States, 131 S. Ct. 2419, 2426 (2011) (internal quotation marks omitted). Neither a "personal constitutional right" nor a means to "redress the injury" of an unconstitutional search, the exclusionary rule is designed to deter future Fourth Amendment violations. Id. (internal

quotation marks omitted). Because the remedy exacts a heavy toll on the justice system, however, the exclusionary rule does not apply whenever suppressing evidence "might provide marginal deterrence." Herring v. United States, 555 U.S. 135, 141 (2009) (internal quotation marks omitted). The rule's corrective value justifies its cost when the police "exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights." United States v. Stokes, 733 F.3d 438, 443 (2d Cir. 2013) (internal quotation marks and citation omitted). But when police act with "an objectively reasonable good-faith belief that their conduct is lawful," or when their conduct involves only "simple, isolated negligence," exclusion simply "cannot pay its way." Davis, 131 S. Ct. at 2427-28 (internal quotation marks omitted).

In light of this principle, courts have recognized that evidence obtained by officers "in objectively reasonable reliance" on a warrant subsequently invalidated by a reviewing court is not generally subject to exclusion. See Falso, 544 F.3d at 125 (internal quotation marks omitted). When an officer genuinely believes that he has obtained a valid warrant from a magistrate and executes that warrant in good faith, there is no conscious violation of the Fourth Amendment, "and thus nothing to deter." United States v. Leon, 468 U.S. 897, 920-21 (1984).

To claim the benefits of the good faith exception, however, the officer's reliance on the duly issued warrant "must be objectively reasonable." Id. at 922. Accordingly, the good faith exception cannot shield even an officer who relies on a duly issued warrant in at least four circumstances: "(1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable." United States v. Clark, 638 F.3d 89, 100 (2d Cir. 2011) (internal quotation marks omitted). The Supreme Court has since clarified that these limitations apply not merely in cases of deliberate police misconduct, but also in situations where an officer is "reckless" or "grossly negligent" in seeking or executing a warrant. Herring, 555 U.S. at 144; see also Davis, 131 S. Ct. at 2427.[5]

[5] The government suggests that "gross negligence" vitiates the good faith exception only where an officer conducts a warrantless search, but not where he relies on a warrant. We have never recognized such a distinction. From its inception in Leon, the good faith exception has always presumed that the challenged search may have relied on a duly issued warrant. See 468 U.S. at 920-21. Accordingly, we can presume that the "basic insight of the Leon line of cases" that exclusion should be limited to cases of "deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights," Davis, 131 S. Ct. at 2427 (internal quotation marks omitted), applies equally to searches conducted with or

While denying that Agent Ouzer "intentionally" misled the magistrate judge, the district court found that Agent Ouzer's affidavit was so "grossly negligent" as to preclude the good faith exception. Specifically, the court noted (1) that Agent Ouzer's knowledge of the suppression ruling in Coon should have alerted him to the staleness of his evidence; (2) that his affidavit "significantly exaggerated the credible import" of the IP logs; and (3) that his affidavit baselessly claimed that the suspect was involved in the "distribution" of child pornography. On appeal, Raymonda adds that Agent Ouzer omitted the critical fact that all GET requests from www.coolib.org occurred in the span of seventeen seconds.[6]

Accepting the district court's factual findings and taking Raymonda's

---

without a warrant. While we have never directly clarified this principle, our sister Circuits commonly list an officer's "gross negligence" as sufficient grounds for excluding evidence discovered through a subsequently invalidated warrant. See, e.g., United States v. Sedaghaty, 728 F.3d 885, 926 (9th Cir. 2013); United States v. Campbell, 603 F.3d 1218, 1225-26 (10th Cir. 2010); United States v. Allen, 625 F.3d 830, 840 (5th Cir. 2010); United States v. Master, 614 F.3d 236, 242 (6th Cir. 2010); United States v. Tracey, 597 F.3d 140, 154 (3d Cir. 2010).

[6] Raymonda's initial motion to suppress claimed that the agents were not entitled to the good faith exception not only because of Agent Ouzer's misleading representations in the affidavit, but also because of an alleged facial lack of probable cause. The district court relied purely on the former ground, and Raymonda presses only that argument on appeal.

additional argument into account, we cannot find that these facts add up to gross negligence. As to Agent Ouzer's involvement in Coon, as a matter of law, a prior holding by a district court cannot establish a binding principle of law sufficient to undermine an agent's good faith reliance on a later warrant. The good faith exception's requirement that an officer act with "objective reliance" on a magistrate's warrant demands only that the officer exhibit "reasonable knowledge of what the law prohibits." United States v. George, 975 F.2d 72, 77 (2d Cir. 1992); see also Leon, 468 U.S. at 919 ("[E]vidence obtained from a search should be suppressed only if . . . the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional . . . .") (internal quotation marks omitted). Where a relevant legal deficiency "was not previously established in precedent," the agent's failure to recognize that deficiency cannot vitiate good faith. Clark, 638 F.3d at 105. Because district court decisions "create no rule of law binding on other courts," ATSI Commc'ns, Inc. v. Shaar Fund, Ltd, 547 F.3d 109, 112 (2d Cir. 2008), Agent Ouzer's knowledge that Coon found nearly year-old evidence of possession too stale to create probable cause cannot have given him notice that his affidavit in

this case would be found equally deficient.[7]

Similarly, Agent Ouzer's conclusory statement that Raymonda "exhibit[ed] common characteristics . . . of someone involved in the distribution, receipt, and possession of child pornography" can hardly have misled the magistrate judge. An isolated boilerplate remark following an extensive recitation of the evidence concerning Raymonda, which consisted exclusively of IP logs showing that the suspect accessed and viewed thumbnails of child pornography, that statement did not plausibly suggest the existence of additional evidence, not otherwise disclosed in the affidavit, that the suspect actually distributed child pornography. At most, it suggested the agent's belief that the suspect's online activities in this case conformed with patterns common to those interested in the receipt and possession of child pornography – as well as in the distribution of child pornography – more broadly. Considering the remark's entirely conclusory nature, there is no likelihood that the magistrate judge relied on it to find probable cause. See Gates, 462 U.S. at 239 (holding that "a wholly conclusory

[7] Even had Agent Ouzer thought to connect the cases, Coon is distinguishable on its facts, involving the possession of a single download of child pornography "almost a full year" before the warrant issued. 2011 WL 1871165, at *1-*2. And even there the district court observed that "this is an exceptionally close case." Id. at *4.

statement . . . failed" to "provide the magistrate judge with a substantial basis for determining the existence of probable cause").

Thus, any claim that Agent Ouzer negligently misled the magistrate judge must rest on his apparently inadvertent mischaracterizations of the IP logs: his suggestion that the suspect intentionally accessed 76 pornographic images and his omission of the fact that the GET requests all occurred within seventeen seconds. With regard to the seventeen-second span, we note that the IP logs provided by Agent Sajo did not list the GET requests in chronological order, but rather consisted of 76 seemingly arbitrary lines of data. While a conscientious investigator might have taken the initiative to analyze this data for the precise download period, we cannot find Agent Ouzer "grossly negligent" for failing to anticipate the work of Raymonda's expert witness and sift through all 76 entries to compare the varying time stamps.[8]

---

[8] In addition to insisting that Agent Ouzer "should have" performed such an analysis, see Dissent at 10, the dissent repeatedly implies that Agent Ouzer in fact knew of the seventeen-second span at the time he drafted his affidavit. We find nothing in the record to support that characterization.

We also respectfully disagree with a number of the dissent's additional suggestions that Agent Ouzer deliberately misrepresented facts to the magistrate judge. While the dissent implies that Agent Ouzer willfully misrepresented how long thumbnail images could have been expected to remain on Raymonda's computer and "tried to convey" a false "impression" about Raymonda's

Nor are Agent Ouzer's potential mischaracterizations of the IP logs sufficiently egregious to justify exclusion. As the district court noted, Agent Ouzer did not recklessly or even carelessly include false information in his affidavit, but rather genuinely believed that the GET requests revealed that Raymonda "clicked" to view the thumbnail images. We have no grounds on this record to believe that Agent Ouzer's misunderstanding amounted to a gross lapse in his expected competence in interpreting computer data. More to the point, while Agent Ouzer did misstate that the IP log "provide[d] evidence that the user *intended* to view the content," J. App'x at 50 (emphasis added), his remaining observations that the user of the IP address "accessed," "obtained," and "successfully viewed" images of child pornography are arguably consistent with information in the IP logs regarding the browser's successful downloads of the thumbnails. Absent any finding that he intended to deceive the magistrate judge with these statements, we cannot find gross negligence in Agent Ouzer's use of technically correct language that had the potential to confuse a reader

---

deliberate access to individual thumbnails, see Dissent at 4-5, the record reveals that all such statements reflected Agent Ouzer's genuine, if mistaken, interpretation of the IP logs. Both Judge Scott and Chief Judge Skretny explicitly disavowed any suggestion that Agent Ouzer intentionally included misleading information in his affidavit.

unfamiliar with IP protocol.

We do not doubt that certain statements in Agent Ouzer's affidavit may have exaggerated the significance of his evidence, nor that such statements may have contributed to the issuance of an invalid search warrant. But the exclusionary rule is designed not to redress minor overstatements or simple negligence by the police, but to deter deliberate, reckless, or otherwise inexcusable violations. See Davis, 131 S. Ct. at 2426, 2428. Because Agent Ouzer's oversights in drafting the affidavit fall short of deliberate deception or gross negligence, the good faith exception applies, and precludes suppression of the evidence obtained pursuant to the warrant.[9]

CONCLUSION

The trade in child pornography is a particularly vile aspect of the Internet, and the government's investigations of that traffic are important and delicate ones. Such investigations appropriately rely on specialized information about the propensities of persons interested in child pornography. Yet there are limits to the inferences that can be drawn from that information. Where the only

[9] Because Raymonda's statements to Agent Ouzer proceeded directly from the search warrant, our holding applies to his statements as well as to the physical evidence seized from his home.

evidence supporting a search warrant is equally consistent with a suspect's innocent stumble on an illicit website as with his deliberate access to child pornography, such evidence does not support an inference that the suspect is a "collector" likely to hoard pornographic images past the time that his computer would overwrite the images in the ordinary course.

Because, however, a magistrate judge in this case reached an independent determination of probable cause to search the suspect's home that was not contrary to established law or facially insufficient, and because any errors in the affidavit supporting the warrant application were neither intentionally false nor grossly negligent, the agents were entitled to rely in good faith on the duly issued warrant. Accordingly, the district court erred in suppressing the evidence.

For the foregoing reasons, the district court's order granting Raymonda's suppression motion is REVERSED and the case is remanded to the district court for further proceedings.