United States Court of Appeals
For the First Circuit

No. 24-1889

UNITED STATES OF AMERICA,

Appellee,

v.

ROBERT DAIGLE,

Defendant, Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

[Hon. Nathaniel M. Gorton, U.S. District Judge]

Before

Barron, Chief Judge,
Lipez and Rikelman, Circuit Judges.

Zainabu Rumala, Assistant Federal Public Defender, for appellant.

Randall E. Kromm, Assistant United States Attorney, with whom Leah B. Foley, United States Attorney, was on brief, for appellee.

June 10, 2026

RIKELMAN, Circuit Judge. Robert Daigle appeals the denial of his motion to suppress evidence discovered in a search of his home. According to Daigle, the government did not establish probable cause to believe that child pornography would be found on his home computer at the time of the search. The district court concluded otherwise, relying on facts showing that, nine months earlier, a computer with an IP address tied to Daigle's residence had logged requests on a specialized network for three electronic files that contained child pornography, all within ten minutes. We conclude that these facts were sufficient to meet the probable cause standard and thus affirm.

I. BACKGROUND

A. Relevant Facts

This case arises from a decade-long investigation by law enforcement into Freenet, a peer-to-peer network that "allows users to anonymously share files, chat on message boards, and access websites within the network." To put the legal issues in context, we recount the basic mechanics of Freenet, as well as the events that led the government to Daigle. We draw the facts from the search warrant affidavit submitted in this case by Special Agent Brian O'Sullivan of the Federal Bureau of Investigation (FBI).

1. The Mechanics of Freenet

To access the Freenet network, "a user must first download the Freenet software, which is free and publicly available." A computer running the Freenet software "connects directly to other computers running Freenet, which are called its 'peers.'" When a user installs Freenet, they "agree[] to provide to the network a portion of the storage space on [their] computer hard drive, so that files uploaded by Freenet users can be distributed and stored across the network."

Once a user uploads a file to Freenet, "the software breaks the file into pieces (called 'blocks') and encrypts each piece." These encrypted blocks are then "distributed randomly" and stored by peer computers. Freenet creates an "index piece," which contains a list of all the file's blocks, and assigns a "unique key -- a series of letters, numbers and special characters" -- to the file.

To download a file on Freenet, a user must have the key associated with that file. When a user tries to download a file, Freenet requests that file's blocks from other computers running the Freenet software (the peers). Instead of requesting all the blocks from one peer, Freenet "divide[s] up" the block requests "in roughly equal amounts among the user's peers." If a peer computer does not have the requested blocks, that peer will divide up the request and ask additional peers for the missing blocks,

and so on. Critically, just because a user requests a file does not guarantee that they can retrieve the blocks for that file or download it.

Freenet's design "attempts to hide" which user uploaded or downloaded a file "by making it difficult to differentiate" between the original requestor of a file and a peer who simply forwarded another peer's request for that file. Still, "Freenet warns its users in multiple ways that it does not guarantee anonymity," including by explaining on its public website that it does not mask a computer's IP address.

Although Freenet is not dedicated to child pornography, users can "advertise and distribute images and videos of child pornography" on the network.[1] Importantly, Freenet does not offer a search function, meaning that a user in search of child pornography must first identify the key for a specific file and then use that key to download the file. To obtain such a key, Freenet users can go to "message boards" on the network, where other users might post messages related to child pornography. These message boards often have labels that are suggestive of the

[1] A peer-reviewed, publicly available academic paper studied 70,000 keys "posted to forums [on Freenet] openly dedicated to child sexual exploitation and confirmed to include known [child pornography] images." Brian N. Levine et al., Statistical Detection of Downloaders in Freenet, Procs. Inst. of Elec. & Elecs. Eng'rs Int'l Workshop on Priv. Eng'g, May 2017, at 8. That study determined that approximately 35% of Freenet's overall traffic related to requests for files using those keys. See id.

sexual exploitation of children. Freenet users can also access websites that only operate within the network, known as "Freesites." Certain Freesites contain viewable images of child pornography, along with keys related to child pornography files.

To support investigations into the sharing of child pornography on Freenet, law enforcement officers have access to a modified version of the Freenet software, which has been loaded onto government computers. This modified version is "nearly identical to Freenet," except that it permits officers to track certain information about each request for file blocks that government computers receive from Freenet users. This information includes the requesting user's IP address.

Law enforcement officers "do not target specific peers on Freenet nor do [they] solicit requests from any peers." Rather, they "collect keys associated with suspected child pornography files" and only investigate Freenet users who use those keys to request files. Officers obtain such keys from Freenet message boards, Freesites, and their prior investigations.

A peer-reviewed, publicly available academic paper describes a mathematical formula for determining whether a request for a file of interest originated from a given computer. See Brian N. Levine et al., Statistical Detection of Downloaders in Freenet, Procs. Inst. of Elec. & Elecs. Eng'rs Int'l Workshop on Priv. Eng'g, May 2017, at 8. Based on his training and experience,

O'Sullivan "believe[d] [the formula] to be a reliable method" for law enforcement officers to use in identifying which computer on the Freenet network initiated a request for child pornography files.

2. The Investigation

Using their modified version of Freenet, law enforcement officers identified a computer with an IP address of 96.230.244.94, which was running the Freenet software. Within a ten-minute timeframe, the user of that computer had requested the blocks of three different files. Officers knew that each of those three files contained child pornography. They had acquired the keys for the three files from various sources: a Freenet message board, a Freesite, and a previous investigation. But they were "not aware of how, or from where, this particular Freenet user obtained [the] key[s] in order to attempt to retrieve the files of interest."

The Freenet user initiated the three file requests on Sunday, April 11, 2021, at 7:10 PM, 7:13 PM, and 7:20 PM. Based on the mathematical formula discussed above, O'Sullivan believed that this Freenet user was "the original requestor" of the three files. Law enforcement officers linked the user's IP address to a computer located in a home in Waltham, Massachusetts, which they subsequently confirmed was Daigle's residence.

As O'Sullivan explained, requesting blocks associated with a file on Freenet is equivalent to a "user attempt[ing] to

download the file's contents from Freenet." Making such an attempt, however, does not mean that the user "retrieved all of the necessary [blocks] to successfully download the file." During their investigation, law enforcement officers were unable to confirm whether the user who had requested the three files on April 11 had in fact downloaded them.

After recounting the steps that led law enforcement officers to Daigle's residence, O'Sullivan described in his affidavit the characteristics common to "consumers" of child pornography. As he explained, these characteristics include collecting and maintaining child pornography materials "for several years" and "go[ing] to great lengths to conceal and protect [those collections] from discovery, theft, and damage." According to O'Sullivan, consumers of child pornography often store their collections in various places, including their computers and digital devices.

Relying on his experience, O'Sullivan recounted that individuals who possess child pornography on one digital storage device are likely to possess it on another device as well. As he put it, this makes it "more likely than not that evidence of [such] access will be found in [the suspect's] home." Ultimately, O'Sullivan believed that a Freenet user at Daigle's residence "likely display[ed] characteristics common to consumers of child pornography."

In his affidavit, O'Sullivan also detailed his training and experience in investigating computer-related crimes generally, including those involving child pornography. He explained that a "computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography." According to O'Sullivan, "a computer user's Internet activities generally leave traces or 'footprints' in the web cache and history files of the browser used," and "[s]uch information is often maintained indefinitely until overwritten by other data." He further described how "[e]lectronic files downloaded to a storage medium can be stored for years at little or no cost" and can be "recovered months or years later" after being deleted. Thus, O'Sullivan attested that there was probable cause to believe that evidence of child pornography would be found on a storage medium at Daigle's residence, even months after the attempted downloads.

The government submitted the search warrant application for Daigle's residence on January 10, 2022, nine months after the requests for the Freenet files at issue. The next day, following authorization from a magistrate judge, law enforcement officers executed the search warrant; during the search, they discovered files containing child pornography.

B. Procedural History

Based on the evidence seized during the search, a grand jury indicted Daigle for receipt of child pornography, in violation

of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1). In March 2024, Daigle moved to suppress all evidence obtained during the January 2022 search.[2] The district court denied Daigle's motion, concluding that O'Sullivan's affidavit established probable cause to believe that a search of Daigle's residence would lead to evidence of child pornography; it also explicitly held that the information in the warrant was not stale. See United States v. Daigle, 731 F. Supp. 3d 168, 171-72 (D. Mass. 2024). Alternatively, the court determined that the good-faith exception to the exclusionary rule would apply, thus permitting the government to rely on the evidence from the search. See id. at 173. Daigle entered a conditional guilty plea, while preserving his right to appeal the ruling denying his motion to suppress.

Daigle then timely appealed.

II. STANDARD OF REVIEW

In evaluating a ruling on a motion to suppress, "[w]e review de novo the district court's legal conclusion about whether a given set of facts amounts to probable cause." United States v. Coleman, 149 F.4th 1, 23 (1st Cir. 2025) (quoting United States v. Gonzalez, 113 F.4th 140, 147 (1st Cir. 2024)). Here, Daigle argued

[2] Daigle also requested an evidentiary hearing pursuant to Franks v. Delaware, 438 U.S. 154, 155-56 (1978), to challenge the veracity of the warrant affidavit. The district court denied his request, and Daigle does not appeal that ruling. See United States v. Daigle, 731 F. Supp. 3d 168, 172-73 (D. Mass. 2024).

in his motion that the search warrant affidavit was insufficient to support a finding of probable cause, and there was no evidentiary hearing of any kind. In such cases, we "accord[] deference to the reasonable inferences" that the magistrate judge issuing the search warrant "may have drawn" from the facts stated in the affidavit. Id. (alteration in original) (quoting United States v. Sylvestre, 78 F.4th 28, 33 (1st Cir. 2023)); see United States v. Cortez, 108 F.4th 1, 7 (1st Cir. 2024).

III. DISCUSSION

Daigle argues that O'Sullivan's affidavit failed to establish probable cause to justify a search of his residence for evidence of child pornography, including because the information in the affidavit was stale. As we explain, we disagree.

A. The Probable Cause Standard

When the government applies for a warrant, it "must demonstrate probable cause to believe that (1) a crime has been committed -- the 'commission' element, and (2) enumerated evidence of the offense will be found at the place searched -- the so-called 'nexus' element." Gonzalez, 113 F.4th at 148 (quoting United States v. Roman, 942 F.3d 43, 50 (1st Cir. 2019)). In evaluating the nexus requirement, "the magistrate judge must 'make a practical, common-sense decision whether, given all the circumstances set forth in the [search warrant] affidavit[,] . . . there is a fair probability that contraband or

evidence of a crime will be found in a particular place.'" Id. (second alteration in original) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)). "Fair probability is less than a more-likely-than not standard." Id.

Both elements of the probable cause inquiry "include a temporal component." Id. (quoting United States v. Zayas-Diaz, 95 F.3d 105, 113 (1st Cir. 1996)). "Thus, the magistrate judge must 'consider the accuracy and reliability of the historical facts related in the affidavit[].'" Id. (quoting Zayas-Diaz, 95 F.3d at 113). In doing so, the magistrate judge "must determine 'whether the totality of the circumstances reasonably inferable from the affidavit[]' establishes a fair probability that evidence of the crime will be found in the place to be searched 'at about the time the search warrant would issue, rather than at some [earlier] time.'" Id. (first alteration in original) (quoting Zayas-Diaz, 95 F.3d at 113).

When the information in an affidavit "establishe[s] probable cause at some point in the past but does not support probable cause at the time of the warrant's issuance," that information is considered "stale." Id. (alteration in original) (quoting United States v. McLellan, 792 F.3d 200, 210 (1st Cir. 2015)). There is no bright-line rule for staleness. In evaluating a staleness claim, "we do not measure the timeliness of information simply by counting the number of days that have elapsed."

McLellan, 792 F.3d at 210 (quoting United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008)). Rather, "we must assess the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information." Id. (quoting Morales-Aldahondo, 524 F.3d at 119).

If probable cause did not exist but a magistrate judge nonetheless authorized the search, then "the evidence obtained from the search is usually suppressed," unless the good-faith exception to the exclusionary rule applies. Gonzalez, 113 F.4th at 148.

B. Analysis

Daigle lodges two specific challenges to the district court's ruling denying his motion to suppress. First, he argues that there was not enough information in the search warrant affidavit to believe that he intentionally accessed child pornography. Second, he contends that the information in the affidavit was stale because it described attempted downloads of child pornography that had occurred nine months earlier. We are not persuaded by either argument.

1. Intentionality

We start with Daigle's contention that the government did not establish probable cause to believe that he intentionally,

rather than coincidentally, attempted to download child pornography.

In making this argument, Daigle emphasizes that the government has never alleged that Freenet's "primary purpose . . . [is] the trading of child pornography." Thus, Daigle maintains, the mere fact that he joined the Freenet network cannot prove that he did so with the intent of accessing child pornography. Daigle also points out that a Freenet user can request a file without knowing the contents of that file, given that a key is not attached to a thumbnail or hyperlink that would reveal the file's contents. Although a key could contain a term suggestive of child pornography (for example, "lolita"), he emphasizes that the warrant affidavit does not mention any such terms associated with the keys that he used. He also highlights that the affidavit provides no information about how he obtained the keys. Finally, Daigle reiterates the government's concession that requesting a file on Freenet does not guarantee that a user will retrieve all the blocks for that file such that they can successfully download it.

To be sure, Daigle raises valid points about the features of Freenet and the limits of the information in the government's search warrant application. But in framing his arguments on appeal, Daigle does not fully grapple with the applicable legal standard.

As we have repeatedly held, probable cause requires only a "fair probability" that evidence of the crime will be found in the place to be searched. Gonzalez, 113 F.4th at 148. In determining whether that standard has been met, courts must evaluate the totality of the information presented by the government through the lens of common sense. See id. And "an officer [need not] rule out potentially innocent explanations for every piece of evidence before reaching a reasonable conclusion that there is probable cause." United States v. Flores, 888 F.3d 537, 545 (1st Cir. 2018).

The facts here showed that a Freenet user at Daigle's residence initiated three requests to download three separate files, each of which the government knew to contain child pornography, all within ten minutes. The facts also indicated that Freenet requires a user to engage in a complicated, multi-step process to request a file. On this record, we see no error by the district court in concluding that the unique features of Freenet, combined with the multiple requests within a short period of time, supported a fair probability that "a [Freenet] user at [Daigle's] residence intentionally requested the files to gain access to child pornography." Daigle, 731 F. Supp. 3d at 171. That it remained possible that this user's actions were innocent and unrelated to viewing child pornography does not undercut that conclusion.

In urging us to reverse the district court's ruling, Daigle relies heavily on United States v. Falso, 544 F.3d 110 (2d Cir. 2008), but the facts of that case are distinct in important ways. In Falso, the U.S. Court of Appeals for the Second Circuit found that the FBI agent's "inconclusive statements" about whether the defendant had accessed or even attempted to access a publicly available website featuring child pornography "f[ell] short of establishing probable cause." Id. at 121. As the Second Circuit reasoned, even if it inferred that Falso had accessed the website, the affidavit lacked any allegation that the defendant had "accessed, viewed or downloaded child pornography." Id. Likewise, the court observed, the affidavit failed to offer particular "details about the features and nature of the . . . site," including "whether the [child pornography] images were prominently displayed or required an additional click of the mouse" or "were downloadable." Id.

Because the affidavit here, like the one in Falso, did not state that Daigle viewed or successfully downloaded the child pornography files, Daigle argues that it could not establish probable cause. But unlike the "inconclusive" statements by the FBI agent in Falso, id., O'Sullivan specified that a Freenet user at Daigle's residence had requested three files that the government knew contained child pornography, all within ten minutes. O'Sullivan also provided a thorough description of Freenet's

unique "features and nature," id., including the multi-step process for requesting a file and that a Freenet user would need to obtain the file's key before requesting it. Those facts, taken together, tended to negate the conclusion that the user in question had accidentally stumbled onto the files. Thus, the totality of the circumstances created a fair probability that the user had attempted to download child pornography.

Daigle also argues that the district court erred by factoring the anonymity of Freenet into its analysis, but, again, we disagree. The court explained that "the anonymized nature of Freenet . . . enhance[d] the probability that a user at [Daigle's] residence sought child pornography and not some other innocuous material." Daigle, 731 F. Supp. 3d at 171. In doing so, the court cited our decision in United States v. Anzalone, 923 F.3d 1 (1st Cir. 2019), which concerned the FBI's investigation into Playpen, an online forum that permitted users to distribute child pornography. See id. at 2. In Anzalone, we held that "the totality of the information asserted in the warrant affidavit -- Playpen's hidden nature . . . , its registration requirement, its focus on anonymity, and the image depicted on its homepage -- established the fair probability that users went into Playpen to access child pornography." Id. at 5.

Daigle maintains that Anzalone is off point because, unlike Playpen, Freenet "is not hidden" but publicly available, it

"does not require registration," and it "has no imagery indicating illicit material." In Daigle's words, "the promise of anonymity" on Freenet "does not equate to ill intent."

But Daigle acknowledges that we "did not focus solely on the anonymous nature of Playpen in affirming the probable cause finding" in Anzalone. Likewise, the district court here noted that Freenet's anonymity was "independently insufficient to establish probable cause." Daigle, 731 F. Supp. 3d at 171. In fact, the court devoted only one sentence of its analysis to Freenet's anonymity and instead focused on the circumstances as a whole. See id.

Just as importantly, we rejected the claim in Anzalone that a court should treat as "not indicative of criminality" the fact that online users had to "take several . . . affirmative steps to locate Playpen." 923 F.3d at 5 (emphasis added). As we explained, the defendant's argument overlooked that probable cause "hinge[s] not on discrete pieces of standalone evidence, but on the totality of circumstances." Id. Here, the "affirmative steps" that a Freenet user would need to take to access a child pornography file -- downloading the Freenet software, obtaining the specific key for that file without the benefit of a search function, and making block requests from peers -- are important aspects of the overall probable cause picture.

Based on the totality of the circumstances, we agree with the district court that "it was reasonable for investigators to infer that three separate requests for three different files known to contain child pornography within a short timeframe [indicated more than] mere coincidence." Daigle, 731 F. Supp. 3d at 171.

2. Staleness

Next, Daigle contends that the information in the search warrant affidavit was stale and thus could not prop up a finding of probable cause. To support his argument, he points to the nine-month gap between the download requests on Freenet and the search warrant application. In his view, even if the facts alleged in the affidavit could support a conclusion that he intentionally requested child pornography files on Freenet, those facts were insufficient to permit the conclusion that he would have those files nine months later.

Although Daigle concedes that "the passage of time alone does not necessarily render information stale," he maintains that O'Sullivan's affidavit lacked specific facts indicating that child pornography would "still [be] located" in his home at the time of the search. According to Daigle, his "limited encounter with child pornography" on Freenet was not enough to conclude that he was a consumer of child pornography, which in turn undermined any inference that he would retain illicit materials indefinitely.

On the record here, we cannot agree with Daigle's staleness arguments. In our view, the totality of the facts in O'Sullivan's affidavit added up to a fair probability that Daigle was a consumer of child pornography. That Daigle engaged in a multi-step process to request, in quick succession, three files known to the government to contain child pornography adequately indicated an intent to download illicit materials. From this activity, it was reasonable for the district court to infer that he was a collector of child pornography who would store such materials. See Morales-Aldahondo, 524 F.3d at 118-19 (holding that three-year-old information was not stale in light of agent's testimony that "a person who uses a computer to access child pornography is likely to use his computer both to augment and to store the collected images"); see also McLellan, 792 F.3d at 209 n.5 ("[C]ourts have held time and time again that child pornography traders and collectors maintain their collections for long periods of time, and often store [them] in safe, close, and easily accessible locations.").

In arguing to the contrary, Daigle relies heavily on United States v. Raymonda, 780 F.3d 105 (2d Cir. 2015), but that case does not help his position. To be sure, the Second Circuit agreed with the defendant's staleness argument in Raymonda. See id. at 117. As the court pointed out, the affidavit supporting the search warrant application "contained no evidence" that the

suspect "had deliberately sought to view [certain] thumbnails" of child pornography on a particular website "or that he discovered [that website] while searching for child pornography." Id. at 117. Indeed, the government agent who applied for the warrant "only uncovered the website through an innocuous link on the message board of another site not explicitly associated with child pornography." Id. Thus, the Second Circuit reasoned, the facts in the case were "at least equally consistent with an innocent user inadvertently stumbling upon a child pornography website, being horrified at what he saw, and promptly closing the window." Id. "Under those circumstances, absent any indicia that the suspect was a collector of child pornography likely to hoard pornographic files," the court concluded that a "single incident of access" was not enough to justify a search of the suspect's computer more than nine months later. Id.

The facts of this case are different. Critically, the affidavit here supports the conclusion that Daigle did not "innocent[ly] stumble" upon the child pornography files on Freenet. Id. at 121. Rather, O'Sullivan detailed the involved, multi-step process for requesting such files on the network. This complicated process "tend[ed] to negate the possibility that [Daigle's] brush with child pornography was a purely negligent or inadvertent encounter." Id. at 115. Indeed, as the Second Circuit recognized in Raymonda, courts have found probable cause (and

rejected staleness arguments) based on "a single incident of possession or receipt . . . [when] 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." Id. (emphasis added).

Daigle next points to United States v. Weber, 923 F.2d 1338 (9th Cir. 1990), to shore up his argument, but that case is also readily distinguishable. Weber is not a staleness case per se, but Daigle relies on it for the principle that O'Sullivan's statements about the habits of consumers of child pornography cannot be relevant to the staleness analysis when the government has failed to show that he is such a consumer. The evidence in Weber that the defendant was a consumer of child pornography, however, was much weaker than the evidence here. The U.S. Court of Appeals for the Ninth Circuit noted that, although the search warrant affidavit described how the defendant had received advertising materials that "apparently" contained child pornography years earlier, the affidavit did not suggest that he had requested those materials. Id. at 1344. The court was also unmoved by the fact that the defendant had "answered a government-generated advertisement for child pornography and ordered materials," because those materials would not be delivered until "just before" the warrant's execution. Id. Those facts aside, the court described the affidavit as offering "rambling

boilerplate recitations" about "the habits ascribed to" child pornography collectors, without tying the defendant's own conduct to those habits. Id. at 1345. Thus, the court concluded that probable cause for the search was lacking.

By contrast, O'Sullivan's affidavit did not rest on such shaky ground. Rather, the totality of the information in the affidavit -- that Daigle attempted to download three child pornography files within ten minutes -- permitted the reasonable inference that he was a consumer of child pornography. Because there were enough facts to conclude that Daigle was a consumer of child pornography, it was reasonable to infer that he would collect and then store child pornography materials nine months after the attempted downloads on Freenet.

But even if we disagreed that the facts demonstrated a fair probability that Daigle was a consumer of child pornography, there was enough information in the affidavit to conclude that his computer would yield relevant digital evidence nine months later. When discussing computer-related crimes, O'Sullivan described at length how files downloaded to a computer can be stored indefinitely and recovered months, even years, after being deleted. Given the durability of digital evidence, it was reasonable to infer that evidence of the requests for the child pornography files would remain on Daigle's computer many months later. See United States v. Vosburgh, 602 F.3d 512, 529 (3d Cir.

2010) (explaining that "information concerning [child pornography] crimes has a relatively long shelf life" and thus "should not be . . . quickly deemed stale," "especially" when "the crime in question is accomplished through the use of a computer" because "computers have long memories" (citation modified)); see also United States v. Gourde, 440 F.3d 1065, 1071 (9th Cir. 2006) (en banc) (rejecting defendant's staleness argument based on four-month delay in executing search warrant because, "[t]hanks to the long memory of computers, any evidence of a crime was almost certainly still on his computer, even if he had tried to delete the images").

Indeed, we have previously rejected staleness claims in similar cases that involved more than nine months of delay. See, e.g., Morales-Aldahondo, 524 F.3d at 119 (rejecting defendant's staleness argument when more than three years had elapsed between his downloads of child pornography materials to his computer and the warrant application). Thus, we see no error in the district court's conclusion that there was a fair probability that digital evidence related to the requested files would remain on Daigle's computer nine months after the download requests on Freenet.[3]

[3] Because we determine that there was probable cause to support the search warrant, we do not address Daigle's argument challenging the district court's alternative ruling denying his motion to suppress based on the good-faith exception to the exclusionary rule. See McLellan, 792 F.3d at 207 n.4 ("Because we

IV. CONCLUSION

For all these reasons, we **affirm** the district court's ruling denying Daigle's motion to suppress.

---

agree with the district court on the merits, we do not review [its] alternate holding [that the FBI acted in good faith].").