PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,
v.
THOMAS MCCOY RICHARDSON, JR.,
Defendant-Appellant.

AOL LLC,
Amicus Supporting Appellee.

No. 09-4072

Appeal from the United States District Court
for the Western District of North Carolina, at Charlotte.
Martin K. Reidinger, District Judge.
(3:06-cr-00085-MR-1)

Argued: March 24, 2010

Decided: June 11, 2010

Before TRAXLER, Chief Judge, and WILKINSON and DUNCAN, Circuit Judges.

Affirmed by published opinion. Chief Judge Traxler wrote the opinion, in which Judge Wilkinson and Judge Duncan joined.

COUNSEL

ARGUED: Anthony Glen Scheer, RAWLS, DICKINSON & SCHEER, PA, Charlotte, North Carolina, for Appellant. Amy Elizabeth Ray, OFFICE OF THE UNITED STATES ATTORNEY, Asheville, North Carolina, for Appellee. **ON BRIEF**: Edward R. Ryan, United States Attorney, Charlotte, North Carolina, for Appellee. Christopher G. Bubb, Vice President, General Counsel, John R. LoGalbo, Assistant General Counsel, AOL LLC, Dulles, Virginia, for Amicus Supporting Appellee.

OPINION

TRAXLER, Chief Judge:

Thomas McCoy Richardson, Jr., pled guilty to violating 18 U.S.C. § 2252A(a)(1) & (b)(1) by "knowingly transport[ing] and ship[ping] in interstate and foreign commerce, by means of a computer, child pornography," J.A. 16, and to violating 18 U.S.C. § 2252A(a)(5) by "knowingly possess[ing] material that contained images of child pornography," J.A. 16. In doing so, Richardson preserved the right to appeal the district court's order denying his motion to suppress and quashing his subpoena duces tecum under Rule 17(c)(2) of the Federal Rules of Criminal Procedure.

On appeal, Richardson contends that AOL LLC ("AOL"), an internet service provider ("ISP") with whom he had an e-mail account, discovered the illegal images on which Richardson's child pornography charges were based by conducting an unconstitutional search on behalf of the Government. Richardson also contends that the search warrant subsequently executed at his Charlotte-area apartment was not supported by probable cause, rendering the evidence culled from his computer inadmissible. Finally, Richardson claims that the district

court committed reversible error in granting AOL's motion to quash his subpoena seeking the production of documents that would establish an agency relationship between AOL and the Government with respect to the detection of AOL subscribers involved in child pornography. We conclude that the district court correctly rejected these arguments and affirm the district court.

I.

On June 10, 2004, AOL, pursuant to a mandatory reporting requirement set forth in 42 U.S.C. § 13032(b)(1),[1] reported to the Cyber Tip Line at the National Center for Missing and Exploited Children ("NCMEC") that AOL had detected the transmission of child pornography images by a subscriber using an e-mail address called knifeisland@aol.com. NCMEC, also as mandated by the same federal law, passed along this information to the North Carolina State Bureau of Investigation ("SBI"), which, in turn, served AOL with an administrative subpoena for subscriber information related to the "knifeisland@aol.com" address. AOL determined that the "knifeisland@aol.com" account was registered to Richardson at 2541 Pine View Lane, Apartment H, Gastonia, North Carolina. The screen name "tr2066" was also linked to this account. By August 2004, however, when SBI agents received and followed up on this information, Richardson no longer resided at the 2541 Pine View Lane address and no forwarding address was available.

The investigation of Richardson apparently stalled for about one year. Then, on September 2, 2005, AOL reported to NCMEC that it had detected the transmission of two e-mail messages containing images depicting child pornography from an account named "tr1029@aol.com" by a person using the screen name "tr1029." NCSBI Agent J.D. White initiated

[1]This particular provision is no longer in effect. The reporting requirements were amended and are now codified in 18 U.S.C. § 2258A.

an investigation following this second report. Pursuant to another administrative subpoena, AOL indicated that the "tr1029@aol.com" account was registered to Richardson at 8508 Park Road, Charlotte, North Carolina. The Park Road address, as it turned out, was the location of a UPS store. Further investigation by the NCSBI, however, revealed that Richardson was residing in Charlotte at 7805 Andover Woods Drive, Apartment 604, and linked Richardson through his driver's license to both the Park Road address of the UPS store (where Richardson had apparently received mail for a period of time) and the Pine View Lane address in Gastonia (where Richardson had established the knifeisland@aol.com account).

NCSBI agents researched Richardson's criminal history and discovered that Richardson was a registered sex offender in South Carolina as a result of two 1996 convictions. In the first instance, Richardson was arrested and charged with performing a lewd act upon a child under 14 years of age after he entered a Wal-Mart store in Florence, South Carolina, grabbed the buttocks of a minor girl, and uttered an obscene remark to her. He was ultimately convicted of assault and battery of a high and aggravated nature. In the second instance, Richardson was convicted for exposing himself as he walked through the same Wal-Mart.

On November 17, 2005, Agent White applied for a search warrant to search Richardson's Andover Woods Drive apartment in Charlotte primarily for evidence of Richardson's use of a computer to view, store, and transmit images of child pornography. In support of his probable cause showing, Agent White included the information disclosed by AOL pursuant to the administrative subpoenas and the details of the subsequent investigation conducted by NCSBI. Additionally, Agent White provided a summary of his background in criminal and computer investigation as well as his special training in the "investigation[ ] of child sexual exploitation and child pornography." J.A. 41. Based on his experience, Agent White

indicated "[t]he use of computers to traffic in, trade, or collect child pornography has become one of the preferred methods of obtaining such materials . . . [because computers] provide[ ] a high degree of anonymity in obtaining child pornography . . . [and] a sense of privacy and secrecy not attainable by other media." J.A. 50. White further explained in his affidavit that "[i]ndividuals involved in the possession and transportation of child pornography rarely, if ever, dispose of their sexually explicit materials," which "are extremely valuable to these individuals because of the difficulty, scarcity, expense, and danger involved in their collection." J.A. 50. Noting that even computer files that are deleted from the hard drive can be retrieved through a forensic examination of the computer, White asked the issuing judge to find "probable cause to believe that Thomas Richardson's residence, 7805 Andover Woods Drive, Apartment 604, Charlotte, North Carolina, contains a computer or computers that have been used to communicate with individuals to acquire child pornography; store images of child pornography, and distribute images of child pornography." J.A. 51.

On November 17, 2005, law enforcement officers executed the search warrant for Richardson's Andover Woods apartment. The primary evidence recovered in the search was a computer. Richardson indicated that he was the sole user of the computer and admitted that he had sent and received child pornography by email. Richardson also told officers that he was "addicted to viewing [child pornography] over the Internet, but denied ever meeting or speaking by phone with anyone he met on the Internet under the age of 18." J.A. 211. A forensic examination of Richardson's computer revealed 28 images and 21 video files containing child pornography. Some of these images included depictions of adults engaged in illegal, obscene sexual acts with children between four and nine years of age.

Richardson moved to suppress both the evidence seized in the search of his home and his statements to law enforcement

officers during the search. First, Richardson argued that in reporting the contents of his email, AOL was acting as an agent of the Government and had therefore conducted an unconstitutional warrantless search of his private email communications. Second, Richardson argued that even if AOL had not acted as a law enforcement agent in reporting the emails, the issuing judge lacked probable cause to believe that evidence of a child pornography offense would be located at his apartment at the time of the search.

Subsequently, in hopes of obtaining documentary support for his argument that AOL was acting as an agent for the Government, Richardson served AOL with a subpoena duces tecum pursuant to Rule 17(c)(1) of the Federal Rules of Civil Procedure requesting that AOL produce

> all records (including but not limited to emails, postal correspondence, minutes/notes of meetings, memoranda, and public relations material, and Congressional testimony) relating to AOL's coordination of efforts, training and/or strategic partnerships with all agencies of the United States Department of Justice, the United States Postal Service, the Secret Service, the Internet Crimes Against Children Task Force with the Department of Justice, and the [NCMEC], regarding the detection and reporting of child pornography content in emails and/or web browsing activities by AOL subscribers or on its network.

J.A. 64.

In response to the subpoena, AOL filed a motion to quash on the grounds that the subpoena was grossly overbroad in scope and that "compliance would be unreasonable or oppressive." Fed. R. Crim. P. 17(c)(2). AOL argued that Richardson's subpoena was essentially a fishing expedition "based on the unsupported legal theory that AOL is an *agent* of the

United States," J.A. 58, and that compliance with the subpoena would require AOL "to carry out a search of its immense paper files and data bases seeking that which does not exist." J.A. 60.

In support of its motion to quash, AOL submitted a declaration from AOL Assistant General Counsel John R. LoGalbo primarily to show that there was no agency relationship between AOL and the Government. LoGalbo denied that law enforcement asked AOL to search Richardson's email or otherwise participate in the investigation of Richardson "except through the ordinary forms of compulsory legal process." J.A. 66. Instead, LoGalbo stated, AOL detected the illegal images attached to Richardson's email transmissions through AOL's Image Detection and Filtering Program ("IDFP"), one of several internally-developed scanning programs designed to keep AOL's systems secure. The IDFP, as summarized by the LoGalbo Declaration, recognizes and compares the digital "fingerprint" (known as a "hash value") of a given file attached to a subscriber's email with the digital "fingerprint" of a file that AOL previously identified as containing an image depicting child pornography. LoGalbo indicated that if the IDFP detected a match suggesting that an email transmission contained child pornography images, then AOL notified the NCMEC as required by 42 U.S.C. § 13032. According to LoGalbo, "AOL developed and began using the IDFP in 2002 in order to protect its rights and property against lawbreakers, prevent the network from being used to carry or store contraband (i.e., illegal child pornography), and fulfill its legal obligation to report the transmission . . . of child pornography on its systems." J.A. 65.

The magistrate judge concluded that the subpoena was unreasonably broad and, therefore, that Richardson failed to show that all of the information sought by the subpoena was relevant, admissible, and specific. *See United States v. Nixon*, 418 U.S. 683, 698-700 (1974). The district court adopted the ruling of the magistrate judge.

The magistrate judge then recommended that Richardson's motion to suppress be denied. First, the magistrate judge concluded that the search warrant was supported by probable cause and rejected Richardson's argument that Agent White's affidavit failed to establish a sufficient nexus between evidence of the child pornography offense and the Andover Woods apartment where the warrant was executed. The magistrate judge found that, based both on the allegations specifically related to Richardson and the "general 'profile'" of child pornographers, J.A. 214, "there was a fair probability that the computer used by defendant for transmission of and storage of [child pornography] would be found in his residence." J.A. 213. The district court adopted the recommendation of the magistrate judge.[2]

Second, the magistrate judge rejected Richardson's argument that AOL was acting as an agent for law enforcement and therefore conducted a warrantless search. In concluding that Richardson failed to carry his burden of establishing that AOL served as an agent or instrument of the government, the magistrate judge noted that AOL's "discovery of [child pornography] associated with [Richardson's] email account was the result of routine scanning the company conducts to recognize files that may be detrimental to AOL." J.A. 216. The district court adopted this recommendation as well.

Following the denial of his motion to suppress, Richardson pled guilty to transporting and shipping child pornography in violation of 18 U.S.C. §§ 2252A(a)(1) & (b)(1), and to possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5). Under the terms of his plea agreement, Richardson preserved his right to appeal both the denial of his

[2] The magistrate judge also concluded that even if the warrant lacked probable cause, the good faith exception under *United States v. Leon*, 468 U.S. 897, 913 (1984), would apply. The district court, however, declined to reach the issue of whether the law enforcement officers acted in good faith.

motion to suppress and the granting of AOL's motion to quash.

II.

Richardson believes that AOL, functioning as a government agent, conducted a constitutionally impermissible search when it scanned his email communications for illicit images of child pornography without a search warrant. If AOL was a government agent, then probable cause and a warrant were required before any search was undertaken. If, however, AOL acted in a private capacity, then government activity is not implicated and the Fourth Amendment does not apply.

Assuming that AOL conducted a search within the meaning of the Fourth Amendment, we conclude that AOL's actions did not equate to governmental conduct triggering constitutional protection. The Fourth Amendment guarantees citizens the right to be free from "unreasonable searches and seizures." U.S. Const. amend. IV. But for a few exceptions, warrantless searches and seizures are "*per se* unreasonable." *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973) (internal quotation marks omitted). The Fourth Amendment, however, does not protect against searches, no matter how unreasonable, conducted "by private individuals acting in a private capacity." *United States v. Jarrett*, 338 F.3d 339, 344 (4th Cir. 2003); *see United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Rather, the Fourth Amendment "proscrib[es] only governmental action," *Jacobsen*, 466 U.S. at 113, and thus "evidence secured by private searches, even if illegal, need not be excluded from a criminal trial," *United States v. Ellyson*, 326 F.3d 522, 527 (4th Cir. 2003) (internal quotation marks omitted).

However, when a private individual conducts a search "as an instrument or agent of the Government," *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989), the limits imposed by the Fourth Amendment apply, *see Jarrett*,

338 F.3d at 344 ("The Fourth Amendment protects against unreasonable searches and seizures by Government officials and those private individuals acting as instruments or agents of the Government." (alterations and internal quotation marks omitted)). The defendant shoulders the burden of establishing the existence of an agency relationship—"a fact-intensive inquiry that is guided by common law agency principles." *Ellyson*, 326 F.3d at 527; *see Jarrett*, 338 F.3d at 344.

The question of whether a private entity such as AOL serves as a mere conduit for the Government in performing a search "necessarily turns on the degree of the Government's participation in the private party's activities." *Skinner*, 489 U.S. at 614. "[T]here must be some evidence of Government participation in or affirmative encouragement of the private search before a court will hold it unconstitutional. Passive acceptance by the Government is not enough." *Jarrett*, 338 F.3d at 346. Additionally, we generally look for evidence bearing upon the question of "whether the private party's purpose for conducting the search was to assist law enforcement efforts or to further h[is] own ends." *Ellyson*, 326 F.3d at 527 (internal quotation marks omitted).

Thus, the key factors bearing upon the question of whether a search by a private person constitutes a Government search are: "(1) whether the Government knew of and acquiesced in the private search; and (2) whether the private individual intended to assist law enforcement or had some other independent motivation." *Jarrett*, 338 F.3d at 344.

There is no question that law enforcement agents did not actually participate in the search at issue here. Richardson does not dispute LoGalbo's assertion that no law enforcement agency specifically asked AOL to search Richardson's email or provided information about Richardson to cause AOL to scan his emails. Neither did law enforcement officials request that AOL aid in the investigation of Richardson "except through the ordinary forms of compulsory legal process," *i.e.*,

"two administrative subpoenas and a preservation request" served pursuant to the Stored Communications Act "for the purpose of identifying the name, address, and other subscriber identifying information for an AOL client." J.A. 66; *see* 18 U.S.C. § 2703. There is nothing in the record to suggest that, in fact, law enforcement agents were involved in the search or investigation of Richardson's email transmissions until after AOL reported its discoveries to NCMEC. Likewise, there is little evidence in this record to suggest that AOL intended to assist the Government in its case against Richardson. Without the unspecified discovery materials to which he believes he is entitled pursuant to the subpoena duces tecum quashed by the district court, Richardson is essentially forced to concede that there is little evidence in this record upon which to demonstrate the existence of a *de facto* agency relationship between AOL and the Government.

Instead, Richardson contends that by mandating AOL's compliance with the reporting scheme set forth in 42 U.S.C. § 13032, the Government actively encouraged the search of his email and transformed AOL into its agent. According to Richardson, the Government, by regulating ISP conduct, did not simply acquiesce to AOL's actions, but instead was actively involved in the search so as to "trigger[ ] Fourth Amendment protections, regardless of the private party's intentions." *Presley v. City of Charlottesville*, 464 F.3d 480, 488 n.7 (4th Cir. 2006).

Richardson draws an analogy to the Supreme Court's decision in *Skinner v. Railway Labor Executives' Association* for the basis of his argument. In *Skinner*, the Court considered whether the regulatory scheme imposed by the Federal Railroad Administration ("FRA") for mandatory and permissive drug testing by private railroads implicated the Fourth Amendment. Subpart C of the regulations, entitled "Post-Accident Toxicological Testing," required railroads to gather blood and urine samples from employees involved in serious accidents resulting in fatalities, injuries or significant property

damage. *See Skinner*, 489 U.S. at 609. Because the regulations in subpart C mandated the means, methods and procedures for testing, the Court concluded that "[a] railroad that complies with the provisions of Subpart C of the regulations does so by compulsion of sovereign authority, and the lawfulness of its acts is controlled by the Fourth Amendment." *Id.* at 614.

A more difficult question for the *Skinner* Court, however, was whether the Fourth Amendment was implicated when a private railroad tested its employees under certain nonmandatory regulations. Subpart D of the FRA's regulatory scheme, entitled "Authorization to Test for Cause," was permissive, authorizing breath or urine tests when a supervisor had a "'reasonable suspicion'" that a worker's actions "contributed to the occurrence or severity of [an] accident" or that an employee was "under the influence of alcohol." *Id.* at 611. Although permissive, Subpart D nevertheless dictated *how* the blood and urine tests were to be conducted: "As in the case of samples procured under Subpart C, the regulations set forth procedures for the collection of samples, and require[d] that samples be analyzed by a method that is reliable within known tolerances." *Id.* at 611-12 (internal quotation marks omitted). Moreover, the regulations "confer[red] upon the FRA the right to receive certain biological samples and test results procured by railroads pursuant to Subpart D." *Id.* at 615.[3]

[3]Subpart D also prescribed formal procedures in the event samples procured under Subpart D were used for disciplinary purposes:

> Subpart D further provides that whenever the results of either breath or urine tests are intended for use in a disciplinary proceeding, the employee must be given the opportunity to provide a blood sample for analysis at an independent medical facility. § 219.303(c). If an employee declines to give a blood sample, the railroad may presume impairment, absent persuasive evidence to the contrary, from a positive showing of controlled substance residues in the urine. The railroad must, however, provide detailed notice of this presumption to its employees, and advise them of their right to provide a contemporaneous blood sample.

Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 611 (1989).

The Court concluded that, despite the non-mandatory nature of Subpart D, a private railroad acts as a government agent when conducting breath or urine tests under that section:

> The fact that the Government has not compelled a private party to perform a search does not, by itself, establish that the search is a private one. Here, specific features of the regulations combine to convince us that the Government did more than adopt a passive position toward the underlying private conduct.

Id. at 615. The Court explained that the Government's intent to actively participate and exert a measure of control over any search under Subpart D was apparent from the fact that the regulations preempted state law and "supersede[d] any provision of a collective bargaining agreement, or arbitration award construing such an agreement." *Id.* (internal quotation marks omitted). Additionally, the Court noted a private railroad was not permitted to "divest itself of, or otherwise compromise by contract, the authority conferred by Subpart D," and its employees were not "free to decline . . . to submit to breath or urine tests under the conditions set forth in Subpart D." *Id.*

Based on those provisions, the Court in *Skinner* concluded that any testing under Subpart D was not "primarily the result of private initiative" and thus triggered application of the Fourth Amendment. *Id.* The regulations in *Skinner* clearly demonstrated "the Government's encouragement, endorsement, and participation," *id.* at 615-16, by "remov[ing] all legal barriers" to such testing, by making clear the Government's "strong preference for testing" and "its desire to share the fruits of such intrusions," and by "mandat[ing] that the railroads not bargain away the authority to perform tests granted by Subpart D." *Id.* at 615.

We reject Richardson's attempt to draw an analogy between the simple reporting requirement of § 13032 and the

regulatory scheme at issue in *Skinner* authorizing a search. The version of § 13032 in effect when AOL reported Richardson required only that an ISP such as AOL report to the Cyber Tip Line at NCMEC in the event it "obtain[ed] knowledge of facts or circumstances from which a violation of section . . . 2252A . . . involving child pornography . . . [wa]s apparent." 42 U.S.C. § 13032(b)(1). Unlike the regulatory scheme at issue in *Skinner*, § 13032(b)(1) neither directed AOL to actively seek evidence of child pornography in certain circumstances nor prescribed the procedures for doing so in the event that AOL decided to ferret out subscribers using its system to transmit illegal digital images. In fact, Congress made abundantly clear that § 13032(b)(1) was not to be interpreted as requiring an ISP to monitor a subscriber's internet activity, explicitly stating that "[n]othing in this section may be construed to require a provider of electronic communication services or remote computing services to engage in the monitoring of any user, subscriber, or customer of that provider, or the content of any communication of any such person." 42 U.S.C. § 13032(e).

The extensive regulatory scheme at issue in *Skinner* suggested a "strong preference for testing," having eliminated "all legal barriers to the testing." *Skinner*, 489 U.S. at 615. Indeed, the FRA's regulatory scheme forbade railroads from contracting away the authority to perform such tests via the collective bargaining process. By contrast, nothing in § 13032 precludes AOL or any other ISP from entering into subscriber agreements that actually preclude monitoring or the use of a scanning tool, nor does any portion of § 13032 remotely suggest a congressional preference for monitoring.

Moreover, the penalty provision for failure to report contained in § 13032 does not persuade us to the contrary. Richardson suggests that ISPs such as AOL would be compelled as a practical matter to monitor their subscribers in the face of substantial monetary fines imposed against "[a] provider . . . who knowingly and willfully fails to make a report" under

§ 13032(b)(1). 42 U.S.C. § 13032(b)(4).[4] As AOL points out, however, the converse is just as likely to be true, if not more so—if substantial fines are imposed for the failure to report known facts suggesting a violation of federal child pornography laws, ISPs and others subject to such penalties might just as well take steps to avoid discovering reportable information.

Finally, we reject Richardson's argument that Congress' intent to deputize ISPs in the Government's effort to fight child pornography on the Internet is reflected by the immunity from civil liability afforded by § 13032(c). *See* 42 U.S.C. § 13032(c) ("No provider or user of an electronic communication service or a remote computing service to the public shall be held liable on account of any action taken in good faith to comply with or pursuant to this section."). Richardson believes this is especially true given the policy statements contained in the Communications Decency Act of a national policy "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material" and "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity . . . by means of computer." 47 U.S.C. §§ 230(b)(4) & (5).

The plain language of § 13032(c) clears the way for ISPs to *report* violations of the child pornography laws, not investigate them. The provision was clearly aimed at immunizing civil claims for mistaken and incorrect reports issued to the NCMEC and in no way encourages surreptitious searches. The Communications Decency Act is likewise of no assistance to Richardson, as it aims "to encourage service providers to self-regulate the dissemination of offensive material over their services" by protecting service providers from law-

[4]An initial failure to report carried a fine of up to $50,000, while a subsequent failure carried a possible fine of $100,000. *See* 42 U.S.C. § 13032(b)(4).

suits casting them "in the role of a publisher." *Zeran v. America Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997).

We conclude that the statutory provision pursuant to which AOL reported Richardson's activities did not effectively convert AOL into an agent of the Government for Fourth Amendment purposes.

III.

We review the district court's order granting AOL's motion to quash under Rule 17(c) of the Federal Rules of Criminal Procedure for an abuse of discretion. *See United States v. Fowler*, 932 F.2d 306, 311 (4th Cir. 1991). In this context, an abuse of discretion occurs when the court uses an erroneous legal standard or bases its decision on clearly erroneous facts. *See United States v. Under Seal (In re Grand Jury)*, 478 F.3d 581, 584 (4th Cir. 2007).

The subpoena duces tecum issued by Richardson to AOL sought the production of essentially any document that would support his theory that AOL was in an agency relationship with the Government:

> YOU ARE . . . COMMANDED to bring with you the following document(s) or object(s): . . . [A]ll records (including but not limited to emails, postal correspondence, minutes/notes of meetings, memoranda, and public relations material, and Congressional testimony) relating to AOL's coordination of efforts, training and/or strategic partnerships with all agencies of the [U.S.] Department of Justice, . . . Postal Service, the Secret Service, the Internet Crimes Against Children Task Force . . . and the [NCMEC], regarding the detection and reporting of child pornography content in emails and/or web browsing activity by AOL subscribers or on its network.

J.A. 64.

Under Rule 17(c)(2), the court "may quash or modify" a subpoena duces tecum "if compliance would be unreasonable or oppressive." Fed. R. Civ. P. 17(c)(2). A subpoena is unreasonable or oppressive if it is "excessively broad" or "overly vague." *In re Grand Jury*, 478 F.3d at 584. In that vein, a fundamental concern is that the subpoena duces tecum is not intended to provide a means of pretrial discovery; rather, its primary purpose is simply "to expedite the trial by providing a time and place *before* trial for the inspection of subpoenaed materials." *Nixon*, 418 U.S. at 689-99; *see Fowler*, 932 F.2d at 311 (rejecting criminal defendant's application for a subpoena duces tecum in that it "was little more than a duplication of [his] discovery motion").

Richardson bears the burden under *Nixon* of showing that the material he has subpoenaed meets the requirements of "(1) relevancy; (2) admissibility; [and] (3) specificity." *Nixon*, 418 U.S. at 700. The subpoena duces tecum must be "made in good faith and [must] not [be] intended as a general 'fishing expedition.'" *Id.*

Richardson contends that any information tending to show a partnership or agency relationship between AOL and the Government was highly relevant to his Fourth Amendment claim and that the district court's refusal to require compliance precluded him from developing this claim. While such information might indeed be relevant, Richardson fails to address the principal deficiency in his subpoena—the lack of specificity. Without it, Richardson is merely fishing for evidence that might support his theory, as if he were in the discovery phase of a civil action. Even on appeal, the phrasing of Richardson's argument—that "he should be allowed to discover the facts" supporting his theory that AOL and the Government were in a partnership—betrays his intention to misuse the subpoena *duces tecum* as a discovery mechanism to develop his agency claim. As we have explained consis-

tently, "a Rule 17 subpoena *duces tecum* cannot substitute for the limited discovery otherwise permitted in criminal cases and the hope of obtaining favorable evidence does not justify the issuance of such a subpoena." *United States v. Caro*, 597 F.3d 608, 620 (4th Cir. 2010) (internal quotation marks omitted).

We conclude, therefore, that the district court did not abuse its discretion in granting AOL's motion to quash.

IV.

Finally, Richardson challenges the district court's conclusion that the search warrant was supported by probable cause. When considering a district court's denial of a suppression motion, we review factual findings for clear error and legal conclusions *de novo*. *See United States v. Blake*, 571 F.3d 331, 338 (4th Cir. 2009), *cert. denied*, 130 S. Ct. 1104 (2010). And, "[a]lthough we review de novo the denial of the motion to suppress by the district court, the determination of probable cause by the issuing magistrate is entitled to great deference from this court." *United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004). Our duty "'is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed.'" *Id.* (quoting *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983)).

Although the concept of probable cause defies a precise definition, it "exist[s] where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found" in the place to be searched. *Ornelas v. United States*, 517 U.S. 690, 696 (1996). A probable cause assessment requires the issuing judge to decide whether, given the totality of the circumstances, there is a "fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238.

Richardson contends that there was no probable cause because the information supporting the issuance of the search warrant was stale. *See United States v. McCall*, 740 F.2d 1331, 1335-36 (4th Cir. 1984) ("A valid search warrant may issue only upon allegations of facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time." (internal quotation marks omitted)); *id.* at 1336 ("[E]vidence seized pursuant to a warrant supported by 'stale' probable cause is not admissible in a criminal trial to establish the defendant's guilt."). In this regard, Richardson claims that the fatal flaw in Agent White's affidavit is that it failed to specify the date on which he possessed or emailed the illegal images; at most, Richardson contends, the supporting affidavit established probable cause that he possessed and distributed child pornography at some unspecified time in the past. Furthermore, Richardson suggests that the only information offered to the issuing judge to "freshen" the probable cause was boilerplate "profile" information about the general tendencies of child pornography collectors, *e.g.*, that "[i]ndividuals involved in the possession and transportation of child pornography rarely, if ever, dispose of their sexually explicit materials" and tend to store their collected materials in their "residence or other secure location to ensure convenient and ready access." J.A. 50. If Agent White's affidavit establishes probable cause, Richardson concludes, then the residence of anyone who has ever possessed or distributed any such materials at some point in the past will be subject to a search so long as the supporting affidavit includes similar boilerplate language. *See United States v. Prideaux-Wentz*, 543 F.3d 954, 957, 958-59 (7th Cir. 2008) (concluding affidavit contained stale information despite description of "'child pornography collector characteristics'" where the government did not identify dates on which illegal images were uploaded and record indicated that images could have been obtained as much as four years prior to the warrant). We cannot agree.

Although "there is no question that time is a crucial element of probable cause," *McCall*, 740 F.2d at 1335, the exis-

tence of probable cause cannot be determined "by simply counting the number of days between the occurrence of the facts supplied and the issuance of the affidavit," *id.* at 1336 (internal quotation marks omitted). Instead, we "look to all the facts and circumstances of the case, including the nature of the unlawful activity alleged, the length of the activity, and the nature of the property to be seized." *Id.* In the context of child pornography cases, courts have largely concluded that a delay—even a substantial delay—between distribution and the issuance of a search warrant does not render the underlying information stale. This consensus rests on the widespread view among the courts—in accord with Agent White's affidavit—that "collectors and distributors of child pornography value their sexually explicit materials highly, 'rarely if ever' dispose of such material, and store it 'for long periods' in a secure place, typically in their homes." *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997); *see United States v. Watzman*, 486 F.3d 1004, 1008 (7th Cir. 2007) (rejecting challenge to probable cause where three months elapsed between the crime and issuance of the warrant where agent testified child pornographers retain their collected materials for long periods of time); *United States v. Gourde*, 440 F.3d 1065, 1072 (9th Cir. 2006) (en banc) (concluding that "[t]he details provided on the use of computers by child pornographers and the collector profile" provided support for a finding of probable cause); *United States v. Riccardi*, 405 F.3d 852, 861 (10th Cir. 2005) (finding probable cause based, in part, on "the observation that possessors often keep electronic copies of child pornography"); *United States v. Lemon*, 590 F.3d 612, 615 (8th Cir. 2010) ("Many courts, including our own, have given substantial weight to testimony from qualified law enforcement agents about the extent to which pedophiles retain child pornography."), *cert. denied*, No. 90-10170, 2010 WL 1531424 (May 17, 2010); *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008) (holding that three-year delay between acquisition of child pornography and application for warrant did not render supporting informa-

tion stale since "customers of child pornography sites do not quickly dispose of their cache"), *cert. denied*, 129 S. Ct. 512 (2008).

Here, the information provided by Agent White established that no more than four months had passed from the time that Richardson emailed an image depicting child pornography using his "tr1029@aol.com" account until the warrant was issued on November 17, 2005. Although Agent White did not supply the precise date of the email transmission, he indicated that the "tr1029@aol.com" account was established by Richardson on July 22, 2005, and the offending email could thus not have been sent before that time. We conclude that a delay of four months does not preclude a finding of probable cause based on staleness in light of the other information supplied by Agent White, including the previous instance in which Richardson used an AOL account to send such images and Agent White's sworn statement that child pornographers "rarely, if ever, dispose of their sexually explicit materials," and that "even if a computer file is deleted from a hard drive or other computer media, a computer expert is still likely to retrieve . . . such files through scientific examination of the computer." J.A. 50.

Richardson raises one other challenge to the search warrant that is closely related to the idea of staleness. He contends that the affidavit failed to include any specific facts suggesting that evidence of these offenses would be found in the Andover Woods apartment. That is, Richardson argues the affidavit failed to establish a nexus with the place to be searched. According to Richardson, the only basis in the supporting affidavit for finding the required nexus to Richardson's Andover Woods apartment was the generic, boilerplate "child pornographer profile." Richardson believes that there must be some "specific" allegation that he was keeping evidence of these crimes at the Andover Woods apartment—for example, that he was using the same computer at the new residence. We disagree.

Richardson's argument ignores the reasonable, common-sense inferences that an issuing magistrate is permitted to draw from the totality of the circumstances in assessing probable cause. As we have observed before, "the nexus between the place to be searched and the items to be seized may be established by the nature of the item and the normal inferences of where one would likely keep such evidence." *United States v. Anderson*, 851 F.2d 727, 729 (4th Cir. 1988). Agent White's affidavit linked Richardson's email accounts, which he used to distribute child pornography, to his previous and current (at the time of the warrant) addresses. The totality of the evidence, including this information, provided the issuing magistrate with a substantial basis for concluding that there was a fair probability that the computer Richardson used to engage in these unlawful activities was kept in his current residence.

V.

For the foregoing reasons, we affirm the order of the district court denying Richardson's motion to suppress and granting AOL's motion to quash the subpoena duces tecum.

AFFIRMED