COURT OF APPEALS
DECISION
DATED AND FILED

May 9, 2019

Sheila T. Reiff
Clerk of Court of Appeals

Appeal No. 2017AP2422-CR **Cir. Ct. No. 2015CF983**

STATE OF WISCONSIN **IN COURT OF APPEALS**
DISTRICT IV

STATE OF WISCONSIN,

PLAINTIFF-RESPONDENT,

V.

DAVID L. LOVELL,

DEFENDANT-APPELLANT.

APPEAL from a judgment of the circuit court for Dane County: NICHOLAS J. McNAMARA, Judge. *Affirmed*.

Before Lundsten, P.J., Blanchard, and Kloppenburg, JJ.

¶1 PER CURIAM. David Lovell appeals a judgment of conviction on five counts of possession of child pornography following a bench trial. Lovell appeals the circuit court's denial of his pretrial request for an order allowing the defense to do the following: forensically analyze the computer that an investigator for the State used to obtain evidence from a digital, "peer-to-peer" network used for file-sharing. The State used the evidence that the investigator obtained from the peer-to-peer network as a basis to obtain a search warrant to search Lovell's home. In executing the search warrant, police obtained the child pornography evidence that formed the basis for the counts of conviction. We reject Lovell's arguments that the circuit court had statutory authority to order the forensic analysis regarding the peer-to-peer network investigation that Lovell requests. As to constitutional authority, we conclude that Lovell has failed to present a non-speculative basis for relief under any constitutional theory that he identifies.

¶2 Lovell also appeals denial of his pretrial motion to suppress the evidence that police seized pursuant to the warrant-authorized search, alleging that the warrant lacked probable cause because the information in the supporting affidavit was stale. On this issue, we conclude that, given the nature of the evidence sought by the warrant, the search warrant was not issued on the basis of stale information. Accordingly, we affirm.[1]

[1] Lovell makes a third argument, which he recognizes we must reject. He seeks to preserve it for a potential review by our supreme court. Lovell contends, contrary to controlling precedent, that WIS. STAT. § 939.617 does not impose a mandatory minimum sentence for a conviction under WIS. STAT. § 948.12. *See* ***State v. Holcomb***, 2016 WI App 70, 371 Wis. 2d 647, 886 N.W.2d 100, *review denied*, 2017 WI 8, 374 Wis. 2d 157, 895 N.W.2d 842; ***State v. Silverstein***, 2017 WI App 64, 378 Wis. 2d 42, 902 N.W.2d 550, *review denied*, 2018 WI 5, 379 Wis. 2d 53, 906 N.W.2d 452. We must reject this argument under ***Cook v. Cook***, 208 Wis. 2d 166, 190, 560 N.W.2d 246 (1997) ("[T]he court of appeals may not overrule, modify or withdraw language from a previously published decision of the court of appeals.").

(continued)

BACKGROUND

¶3 We begin with background regarding peer-to-peer file-sharing networks, as well as background regarding a State investigator's access to one such network to interact with Lovell's device. Then we summarize facts regarding the seizure of warrant-authorized evidence and subsequent proceedings.

Peer-To-Peer File-Sharing Networks

¶4 At least for the particular peer-to-peer network at issue here, anyone with a computer or other internet-navigating device can access the network by using freely available software. The person using the device to access the network is called a "peer," and cannot control who else might access the network. Peers have the ability to download digital files from other peers, although each peer designates which files on his or her own computer are available for sharing. To this extent, a peer-to-peer network is "public" in nature, and files designated for sharing are not located in the "private spaces" of electronic devices. *See* ***State v. Baric***, 2018 WI App 63, ¶21 & n.6, 384 Wis. 2d 359, 919 N.W.2d 221 (peers do "not have an objectively reasonable expectation of privacy in files … publicly shared" through a peer-to-peer network, even though shared files are located on user's electronic device, because the files were placed in a digital folder designated for sharing on the network).

All references to the Wisconsin Statutes are to the 2017-18 version unless otherwise noted.

Recovery Of Peer-To-Peer Evidence

¶5 In 2013, a state law enforcement agent initiated an undercover investigation aimed at identifying persons using the publicly accessible peer-to-peer network described above to share child pornography. The agent used a software program specifically adapted for law enforcement purposes, which we will refer to as Roundup. The warrant affidavit does not indicate that the agent had any form of court-approved warrant authorizing these searches using Roundup on the peer-to-peer network. Instead, the agent essentially averred in the affidavit that he had conducted a public search, because Roundup is capable of accessing only those "areas of a suspect's computer" that the peer-suspect has allowed, using particular software and folders designated for public file sharing.

¶6 On August 17, 2014, the agent used Roundup to establish a peer-to-peer connection with the device of a peer that had been, at some time in the past, "associated" with a file that contained an image listed in a national database used by law enforcement to track child pornography. Through the agent's network connection to this device, the agent downloaded three files that the device then made available to network peers. These files contained what appeared to the agent to be digital images of children engaged in sexually explicit conduct. We will call these three files "the peer-to-peer evidence."[2]

¶7 In addition to the peer-to-peer evidence, the agent used Roundup to determine the Internet Protocol address ("IP address") of the suspect peer's device.

[2] The parties dispute whether the affidavit can be reasonably read to infer that the agent identified additional evidence of child pornography on the suspect device after August 17, 2014. Without resolving this dispute, we assume in Lovell's favor that the affidavit cannot reasonably be read to aver that the agent identified additional incriminating evidence.

An IP address is a unique number assigned by internet service providers to each device that communicates as part of a computer network that uses the internet. *See* ***Baric***, 384 Wis. 2d 359, ¶4 & n.3. Through a subpoena to the pertinent internet service provider, which supplied the IP address, the agent was able to identify Lovell as the alleged subscriber for the suspect IP address, at least for the period March 12, 2014, to February 17, 2015. The service provider also provided Lovell's alleged residential address in Madison.

¶8 In early May 2015, an agent conducted surveillance of the Madison residence, which appeared to confirm that Lovell resided there. Based on a description of the peer-to-peer evidence and how it was obtained using Roundup, an agent applied for, and was granted, a warrant to search Lovell's premises, and to seize and analyze any computers and other digital devices found there for evidence of child pornography. The agent obtained the search warrant on May 11, 2015.

Seizure Of Warrant-Authorized Evidence And Subsequent Proceedings

¶9 Law enforcement agents executed the warrant at Lovell's home on May 13, 2015. They seized a personal laptop computer and an external hard drive. The agents recovered from these devices 10 files consisting of what appeared to the investigators to be sexually explicit pictures of children. We will call this "the warrant-authorized evidence." Based on the warrant-authorized evidence, the State charged Lovell with multiple counts of possession of child pornography. The State did not rely on the peer-to-peer evidence in filing these charges.

¶10 As pertinent to his appeal, Lovell made two pretrial motions, both of which were denied by the circuit court.

¶11 Lovell moved for an order requiring the State to assist a defense investigation into the way in which the State obtained the peer-to-peer evidence, including by permitting a defense expert to test the State's computer. Through such a test, the defense hoped to establish that the State agent used Roundup to make a warrantless intrusion into private file space on Lovell's computer. More specifically, Lovell asked that the court compel the State to allow defense experts to forensically analyze the State's investigative computer, using the same computer and software "settings" as the agent had used, in an attempt to determine the precise nature of the agent's use of Roundup to connect to Lovell's device through the peer-to-peer network to discover the peer-to-peer evidence.

¶12 At a hearing on this motion, Lovell contended that it was possible that the agent used Roundup to access private files on Lovell's device. By private files, Lovell meant files on the hard drive of his device that he had not made available to the peer-to-peer network through placement in a folder or directory designated for sharing on the network. He argued that the significance of the intrusion into his private files would be that, instead of searching publicly available data, the State would have conducted a warrantless, and therefore unreasonable, search of a portion of Lovell's computer where he reasonably expected privacy. The State does not dispute this last point. That is, the parties agree that, if the agent using Roundup accessed Lovell's private files without a warrant or the benefit of some other exception to the Fourth Amendment, this would have been a violation of the Fourth Amendment's protection of Lovell's reasonable expectation of privacy and the resulting search would be unlawful.

¶13 Experts called by Lovell opined that it is possible for someone to design software that could be used to access private file space on a peer's device. However, those experts did not assert that such an intrusion could be

accomplished using Roundup. Rather, they testified that there was only one way for the defense to verify that an intrusion into Lovell's private file space had not happened in this case. That would be to allow the defense to forensically analyze the same government computer and Roundup software used by the agent, with the same "settings" that the agent used when communicating with Lovell's computer.[3]

¶14 The State pointed to an averment in the warrant affidavit to the effect that the agent using Roundup had the ability to access only publicly available files, not private files; private intrusion was simply impossible. Further, the State cross examined one of Lovell's experts, who acknowledged that he did not know whether Roundup could be used to view or download content not contained in a shared folder on the network. In addition, the State noted that it was not seeking to use the peer-to-peer evidence to prove the charges in this case, but instead was prosecuting Lovell strictly based on the warrant-authorized evidence.

¶15 The court denied the request for access to the State computer primarily because the experts called by Lovell were unable to testify that the agent had the ability to access Lovell's private files using Roundup, much less that the agent had in fact done so. The court further expressed concerns regarding its

[3] The parties make reference on appeal to a related production or discovery issue that involves purported logs of the agent's connections to the peer-to-peer network. However, Lovell does not now develop an argument that anything about the logs provides an independent basis for reversal, and the State makes no helpful references to the logs. Explaining further, when Lovell requested the order for forensic analysis, he also requested "any and all logs and reports generated" by the agent's computer relating to its peer-to-peer connection with Lovell's device. At the discovery motion hearing, an expert called by Lovell explained that programs such as Roundup generate "extensive logs" detailing how the program was used and that these logs were necessary for the expert's analysis. Lovell suggests that he did in fact receive some such logs from the State, but asserts that they were insufficient to establish whether the agent intruded into private file space. Neither party has provided us with a basis to pursue the log topic separately.

authority to compel the State to make its computer available for defense analysis, even if the requested investigation could show that the State could and did access Lovell's private files. Lovell renewed this request later in the course of pretrial litigation. The court denied the renewed request.

¶16 Lovell's second pertinent motion sought suppression of the warrant-authorized evidence, on which the State's case is based, on the ground that the warrant lacked probable cause, based on a staleness argument. The court denied this motion, concluding that it was reasonable for the judge issuing the warrant to infer from the affidavit that Lovell's computer contained child pornography more than 8 months after the agent observed the peer-to-peer evidence.

¶17 Lovell was convicted at a bench trial of possessing child pornography based on the warrant-authorized evidence, and now appeals the denial of his two pretrial motions.

DISCUSSION

¶18 We first address denial of the request for an order allowing forensic analysis and then turn to the denial of the motion to suppress the warrant-authorized evidence.

I. Motion To Allow Forensic Analysis

¶19 Lovell argues that the circuit court erred in denying his request for an order allowing forensic analysis of the investigative computer used to establish a peer-to-peer connection to his device through the peer-to-peer network. Specifically, he contends that the court made two legal errors in denying his request: (1) incorrectly concluding that it lacked authority to issue an order based on WIS. STAT. § 971.23; and (2) incorrectly concluding that it lacked authority to

issue an order based on Lovell's constitutional due process right to present a "complete defense." We first explain why we reject Lovell's statutory argument and then why we reject his constitutional argument.

¶20 In addressing these arguments, we interpret and apply both statutes and constitutional principles, which are questions of law that we decide de novo. ***State v. Schaefer***, 2008 WI 25, ¶17, 308 Wis. 2d 279, 746 N.W.2d 457.

WISCONSIN STAT. § 971.23

¶21 Lovell argues that the circuit court had authority to grant his request for forensic analysis of the investigative computer under WIS. STAT. § 971.23, primarily contending that it falls under sub. (5), and perhaps also pointing to the legislative intent that he may contend is evident in the statutory framework of § 971.23. We reject Lovell's statutory argument based on a plain language interpretation and the circumscribed nature of criminal case discovery under the Wisconsin Statutes. As we explain below, the order Lovell seeks would permit analysis that would, if successful, reveal evidence that could allow him to challenge only the peer-to-peer evidence, which the State does not intend to use at trial, and therefore the court lacked authority to issue the order under § 971.23(5).

¶22 In pertinent part, WIS. STAT. § 971.23(5) provides that "the court may order the production of any item of physical evidence *which is intended to be introduced at the trial* for scientific analysis under such terms and conditions as the court prescribes" (emphasis added). As we have suggested, and Lovell concedes, the State never intended to introduce at trial the peer-to-peer evidence, the investigative computer, or the Roundup software into evidence, nor did it intend to introduce the results of the investigative computer's peer-to-peer connection with Lovell's computer. As noted above, the State based its charges

against Lovell exclusively on the warrant-authorized evidence. Therefore, the targets of Lovell's first motion involved only items that were not physical evidence intended to be introduced at trial. *See* ***Schaefer***, 308 Wis. 2d 279, ¶22-23 ("Traditionally, … statutory discovery [under WIS. STAT. § 971.23] is designed to assure fairness at a criminal *trial*.") (emphasis added).

¶23 Lovell does not explicitly identify any statutory basis outside of WIS. STAT. § 971.23(5) that could have provided authority for the circuit court to compel the State to make the investigative computer available to Lovell's experts. It is unclear, but Lovell may intend to argue that he is entitled to the forensic analysis based on production or discovery obligations of the State implicit in the legislative intent evident in the statutory framework of WIS. STAT. § 971.23. However, we see no room for such an argument.

¶24 Accused persons in criminal prosecutions do not have rights to discovery outside the rights specified in discovery statutes or protected by the state and federal constitutions, notably the disclosures required by ***Brady v. Maryland***, 373 U.S. 83, 87 (1963) and its progeny. *See* ***State v. O'Brien***, 223 Wis. 2d 303, 319, 588 N.W.2d 8 (1999) ("Historically, the right to discovery in criminal cases has been limited to that which is provided by statute.") (citing ***State v. Miller***, 35 Wis. 2d 454, 474, 151 N.W.2d 157 (1967)); ***Britton v. State***, 44 Wis. 2d 109, 117, 170 N.W.2d 785 (1969) (drawing distinction between statutorily defined "discovery" and constitutionally required "disclosure"); ***State ex rel. Lynch v. County Court, Branch III***, 82 Wis. 2d 454, 464-67, 262 N.W.2d 773 (1978) (there is no general right to inspect prosecutor's file under statute or constitution). For this reason, to the extent that Lovell argues for a right to access information that is not expressly required to be produced or made available under WIS. STAT.

§ 971.23, all that remains would be his argument that such a right has some constitutional basis. We now turn to this constitutional argument.

Constitutional Right To A "Complete Defense"

¶25 Lovell argues that he was entitled to the requested order based on his constitutional right as an accused to present a "complete defense," under the federal constitution. *See* ***California v. Trombetta***, 467 U.S. 479, 485 (1984) (Due Process Clause's requirement that "criminal prosecutions must comport with prevailing notions of fundamental fairness" requires that "criminal defendants be afforded a meaningful opportunity to present a complete defense"). More specifically, Lovell argues that, because the possibility of prevailing on a suppression motion can be the "central thrust" of a defense, the due process guarantee of the ability to present a "complete defense" is not satisfied unless defendants can obtain court orders to force the State to disclose otherwise unobtainable information that could form the potential basis for a suppression motion. Seen in this light, Lovell argues that the requested forensic analysis is necessary to a "complete defense," because it is the only way for the defense to determine whether the State intruded into private files in his computer, an intrusion which would create a potential ground to suppress the warrant-authorized evidence as the fruit of an unreasonable search in violation of the Fourth Amendment.

¶26 We assume without deciding that Lovell is correct that his due process rights obligate the State to disclose evidence of a violation of Lovell's

Fourth Amendment rights.[4] We reject this argument because, regardless of its legal basis, factually it rests entirely on speculation. That is, the circuit court could reasonably deny his constitutional argument because it had no factual starting point.

¶27 Lovell does not dispute that, if his due process right to present a complete defense imposed an obligation on the State to disclose evidence supporting a suppression motion, disclosure would be required only of evidence that was "material" to potential suppression. In the same way that the State's duty to disclose exculpatory evidence applies only to evidence that is "material to guilt or innocence," *see* ***State v. Harris***, 2004 WI 64, ¶¶12-13, 272 Wis. 2d 80, 680 N.W.2d 737, under Lovell's assumed right the State could be required to disclose only evidence that is material to Lovell's theory of suppression, namely, evidence that the State intruded into his private files. Therefore, Lovell needs to show a "'reasonable probability'" that, had the State disclosed the evidence he seeks, it would have changed the result of his suppression motion. *See* ***id.***, ¶14 (quoting ***United States v. Bagley***, 473 U.S. 667, 682 (1985)). This requirement that the State disclose only evidence that is material to the defense reflects the principle that the Constitution does not obligate prosecutors to allow complete discovery or inspection of all evidence in the control of the government as a matter of routine practice. *See* ***id.***, ¶16 (citing case including ***United States v. Agurs***, 427 U.S. 97, 109-10 (1976); ***Lynch***, 82 Wis. 2d at 463-64); *see also* ***United States v. Stott***, 245 F.3d 890, 901-02 (7th Cir. 2001) (noting cases in which federal circuit courts

[4] The parties do not cite case law that resolves whether a defendant is constitutionally entitled to the disclosure of evidence that relates strictly to a non-exculpatory, pretrial basis to suppress evidence of guilt. From our own limited research, this appears to be an open question.

assume without deciding that ***Brady***'s disclosure requirements apply at suppression hearing, then denying the ***Brady***-like claim on the basis of materiality of nondisclosed evidence to suppression motion).

¶28 Bearing that context in mind, we conclude that Lovell's request rests on mere speculation and therefore is not material to suppression. As explained in the background, his experts conceded that they were unable to say that Roundup could be used to access private files, much less that the State used it in this way in making the connection to Lovell's device on the peer-to-peer network. Lovell points to no direct evidence that the State downloaded the peer-to-peer evidence from privately kept files, but we now turn to what he apparently argues is indirect evidence.

¶29 This involves a confusing argument that Lovell contends is based on indirect evidence that the State downloaded the peer-to-peer evidence from privately kept files. Lovell points to the fact that one of his experts testified that the expert had been unable to recover the peer-to-peer evidence images from any place, public or private, on Lovell's computer, including searching through data that can be left behind by "deleted" files. The notion appears to be that this particular testimony by the expert gave the court a sufficient basis to conclude that there was something amiss in the averments in the search warrant affidavit about how the investigator had used Roundup. It is enough for us to explain that Lovell fails to develop an argument that the purported "missing images" rendered less speculative the possibility that the investigator used Roundup to access private files on Lovell's computer, or rendered less speculative a possible general argument that Roundup did not function as the State avers. There was no testimony that the alleged absence of the inculpatory peer-to-peer images from Lovell's computer provided a basis for surmising that the images, if previously

stored any place on Lovell's computer, were stored in private file space. Contrary to Lovell's contention, we fail to see how he would not have been able to present such affirmative evidence, if it exists, without access to the State's computer. If Lovell knows that the images used to obtain the search warrant were located in unshared files of his computer, there is no indication in the record as to why he could not have presented that supporting evidence to the attention of the court.[5]

¶30 In sum, we conclude that Lovell has failed to identify authority under WIS. STAT. § 971.23 that the circuit court grant his request to order the State to allow his experts to forensically analyze the investigative computer, or to identify a non-speculative basis for that relief under any constitutional theory.

II. Staleness Challenge To Search Warrant

¶31 Lovell argues that the circuit court erroneously exercised its discretion in denying his motion to suppress the warrant-authorized evidence. Specifically, he contends that the warrant lacked probable cause because the information in the supporting affidavit was stale; that is, probable cause was lacking due to the passage of time. He points to the fact that the peer-to-peer evidence was gathered more than 8 months earlier. He contends that the following additional general observations in the affidavit should have been understood by

[5] We further note that the federal cases on which Lovell relies to show that he has sufficiently demonstrated that his request is material to his suppression claim construe Federal Rule of Criminal Procedure 16(a)(1)(E) (granting defendant right to inspect all documents, data in government's possession that are "material to preparing the defense"), and are not based on the Due Process Clause. *See* ***United States v. Budziak***, 697 F.3d 1105, 1111 (9th Cir. 2012); ***United States v. Crowe***, No. 11-CR-1690, 2013 WL 12335320, *3 & n.2 (D.N.M. Apr. 3, 2013). Moreover, for the reasons stated in the text, we decline to follow these cases to the extent that Lovell relies on them to suggest that Lovell's request is material merely because his expert testified that he could not recover the peer-to-peer evidence images from any place on Lovell's computer.

the warrant-authorizing judge to be inaccurate: child pornography collectors tend to hold onto child pornography and "deleted" files can be later recovered by investigators. We reject this argument on the ground that Lovell fails to show that the warrant-issuing judge could not reasonably consider the 8-month-old evidence sufficiently fresh in light of the general observations about the habits of child pornography collectors and the recoverability of "deleted" electronic files.

¶32 "We accord great deference to the warrant-issuing judge's determination of probable cause, and that determination will stand unless the defendant establishes that the facts are clearly insufficient to support a finding of probable cause." ***State v. Multaler***, 2002 WI 35, ¶7, 252 Wis. 2d 54, 643 N.W.2d 437. The issuing judge may rely on "the usual inferences reasonable persons would draw from the facts presented." ***State v. Gralinski***, 2007 WI App 233, ¶24, 306 Wis. 2d 101, 743 N.W.2d 448 (quoting ***State v. Ward***, 2000 WI 3, ¶28, 231 Wis. 2d 723, 604 N.W.2d 517). Under WIS. STAT. § 968.12(1), a search warrant shall issue "if probable cause is shown." To determine whether probable cause exists, a warrant-issuing judge makes a common sense decision, based on the facts alleged in the affidavit, whether there is a fair probability that evidence of a crime will be found in the pertinent place at the pertinent time. *See* ***id.***, ¶¶14-15.

¶33 ***Gralinski*** guides our analysis. In ***Gralinski***, a search warrant application was supported by an affidavit that contained the following allegations: the defendant's credit card and other personal information had been used to purchase access to a website that, in turn, provided access to other sites containing child pornography; in general, data from files may remain on, and be retrievable from, a hard drive after the user deletes the files; and "individuals who are involved with child pornography are unlikely to ever voluntarily dispose of the images they possess," because they view such images "as prized and valuable

materials." ***Id.***, ¶¶5-8. More than 30 months passed between the identification of the defendant's credit card number being used to access the website and the application for the search warrant. ***Id.***, ¶¶5, 7. We explained that a staleness challenge "requires a review 'of the underlying circumstances, whether the activity is of a protracted or continuous nature, the nature of the criminal activity under investigation, and the nature of what is being sought.'" ***Id.***, ¶28 (quoted source omitted).

¶34 Applying that standard, we concluded that, based on the nature of the evidence sought, it was reasonable for the issuing judge to determine that there was probable cause to believe that evidence of the possession of child pornography would be found on Gralinski's computer. ***Id.***, ¶31. This was based on reasonable inferences that the defendant had downloaded child pornography onto his computer and that the downloaded materials could still be found on Gralinski's computer 30 months later. ***Id.***, ¶¶30-31.

¶35 Consistent with ***Gralinski***, the averments in this case could have reasonably led the warrant-issuing judge to conclude that there was a fair probability that a search of Lovell's computer would have uncovered evidence of his possessing child pornography more than 8 months after the discovery of the peer-to-peer evidence. As in ***Gralinski***, the warrant affidavit here contained allegations, which the affiant averred were based on his training and experience, that child pornography collectors have a proclivity to retain illicit images as prized possessions and that a computer can retain images or data from images even after many computer operators would think that they have fully or permanently deleted them.

¶36 Moreover, the individualized facts here were more incriminating than in ***Gralinski*** in multiple respects. The passage of time here was shorter. Further, the instant case involves stronger direct evidence of intentional collection of child pornography: here there was direct detection of child pornography on the suspect device tied to Lovell, in contrast to ***Gralinski***, in which there was merely an inference that the suspect had downloaded illicit materials from a website, based on having membership with a site granting access to sites displaying such materials. *See* ***id.***, ¶¶20, 30-31.

¶37 Citing federal case law as persuasive authority, Lovell asserts that the proclivities of child pornography collectors should be considered irrelevant to the probable cause analysis on the facts here because there was insufficient evidence described in the affidavit to conclude that he was a collector of child pornography. *See* ***United States v. Raymonda***, 780 F.3d 105, 114-15 (2nd Cir. 2015) ("The 'alleged "proclivities" of collectors of child pornography,' … 'are only relevant if there is probable cause to believe that a given defendant is such a collector.'") (quoted source and alterations omitted). This argument based on persuasive authority is unavailing, because the circumstances surrounding the peer-to-peer evidence created a reasonable inference that Lovell collected child pornography. *See* ***id.*** at 114-15 (a single incident of possession or receipt of child pornography—when there is a reasonable inference that suspect accessed child pornography "willfully and deliberately, actively seeking [the pornography] out to satisfy a preexisting predilection"—supports probable cause level determination that a suspect may be a collector). We conclude that the averments here support the reasonable inference that Lovell had sought out and acquired the peer-to-peer evidence (which involved three separate images, each located in a file on his computer) and then intentionally allowed these images to be shared from his

computer with other peers on the network. This was sufficient evidence for the judge to reasonably conclude that Lovell was a collector, not someone who had "brush[ed] with child pornography" in "a purely negligent or inadvertent encounter, the residue of which was long ago expunged." *See* ***id.*** at 115.

¶38 Lovell makes two unavailing arguments based on what he submits are trends in digital technology that undermine averments in the affidavit regarding the recoverability of deleted files. Both rest on factual assertions that he supports only with the experts' reported inability to recover the peer-to-peer evidence from his computer. However, none of this was presented to the warrant-issuing judge, and thus these arguments fail to recognize that we evaluate the judge's probable cause determination based on the averments presented to the judge. *See* ***Gralinski***, 306 Wis. 2d 101, ¶16. Contrary to the implicit premise of these arguments, judges reviewing warrants are not obligated to engage in independent research to test averments in affidavits. Rather, judges may decide to rely on seemingly credible, supported averments of the type provided by the affiant-agent in this case. *See* ***id.*** (warrant-issuing judge may consider "'both the experience and special knowledge of police officers who are applying for search warrants'") (quoted source omitted). And, if Lovell intends to argue that his technological propositions are simply common sense or common knowledge, we reject that argument as unsupported.

¶39 In sum, we conclude that Lovell has failed to meet his burden to show that the warrant-issuing judge clearly lacked probable cause to issue the search warrant.

CONCLUSION

¶40 For these reasons, we affirm the circuit court's denial of Lovell's request for an order permitting forensic analysis of the computer used in the investigation of peer-to-peer network activity and the court's denial of Lovell's motion to suppress.

By the Court.—Judgment affirmed.

This opinion will not be published. *See* WIS. STAT. RULE 809.23(1)(b)5.