In the
United States Court of Appeals
for the Second Circuit

AUGUST TERM 2014
No. 14-1083-cr

UNITED STATES OF AMERICA,
Appellee,

v.

DEREK THOMAS,
Defendant-Appellant.

On Appeal from the United States District Court
for the District of Vermont

ARGUED: JANUARY 15, 2015
DECIDED: JUNE 11, 2015

Before: WINTER, CABRANES, and RAGGI, *Circuit Judges*.

The question presented is whether a search warrant affidavit that relied upon evidence generated by an automated software program provided a substantial basis for a magistrate judge's conclusion that there was probable cause that child pornography would be found on defendant's computer.

We hold that the affidavit at issue sufficiently established probable cause and that defendant's motions to suppress were properly denied.

The judgment of the United States District Court for the District of Vermont (Christina Reiss, *Chief Judge*) is affirmed.

ELIZABETH D. MANN, Tepper Dardeck Levins & Mann, LLP, Rutland, VT, *for Defendant-Appellant.*

NANCY J. CRESWELL (Paul J. Van De Graaf, *on the brief*), Assistant United States Attorneys, *for* Eugenia A.P. Cowles, Acting United States Attorney for the District of Vermont, Burlington, VT, *for Appellee.*

JOSÉ A. CABRANES, *Circuit Judge*:

The question presented is whether a search warrant affidavit that relied upon evidence generated by an automated software program provided a substantial basis for a magistrate judge's conclusion that there was probable cause that child pornography would be found on defendant's computer.

We hold that the affidavit at issue sufficiently established probable cause and that defendant's motions to suppress were properly denied.

The judgment of the United States District Court for the District of Vermont (Christina Reiss, *Chief Judge*) is affirmed.

BACKGROUND

Defendant Derek Thomas appeals from the denial of his motions to suppress the searches of his residence and his computer. Thomas pleaded guilty to the production of child pornography, in violation of 18 U.S.C. § 2251(a),[1] but reserved the right to appeal

[1] Thomas pleaded guilty to the following statute:

> Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any

from two orders of the District Court for the District of Vermont (Christina Reiss, *Chief Judge*) denying his motions to suppress evidence. On March 31, 2014, the District Court sentenced Thomas principally to 180 months' imprisonment and 8 years' supervised release.

Thomas was arrested as part of a joint federal and state law enforcement investigation in Vermont during 2011 and 2012, known as "Operation Greenwave," into potential child pornography offenses committed through the use of peer-to-peer ("P2P") file-sharing software.[2] As part of the investigation, law enforcement

---

> visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

18 U.S.C § 2251(a).

[2] P2P file-sharing is a means of exchanging files (*i.e.*, photos, videos, songs) with other Internet-connected computer users who are also using file-sharing software. The P2P software is generally publicly available for download

relied upon automated software programs to help locate Internet Protocol ("IP") addresses engaged in the possession and distribution of child pornography.[3] The software, designed for and used by law enforcement, was created by a private "data fusion" company called TLO. *United States v. Thomas*, No. 5:12-cr-37, 2013 WL 6000484, at *4 (D. Vt. Nov. 8, 2013). TLO provides a suite of software and other products—known collectively as the Child Protection System ("CPS")—to licensed law enforcement professionals free of charge to investigate child pornography that is collected and distributed over P2P networks. *Id.*

Traditionally, law enforcement officers seek to detect child pornography offenses by manually sending out search queries for illicit material over P2P networks, one-by-one. CPS automates this process by canvassing these public P2P networks, identifying files that contain child pornography, cataloguing this information, and providing law enforcement officers with a list of the online users who are sharing these files over P2P networks.[4] Law enforcement officers can then use that list to focus their investigative efforts on

---

from the Internet and operates on a particular network. *See United States v. Thomas*, No. 5:12-cr-37, 2013 WL 6000484, at *2-3 (D. Vt. Nov. 8, 2013).

[3] An IP address is a numerical identifier assigned to a particular Internet connection used by one or more computer devices.

[4] For more information on the various types of CPS products, their functionality, and their testing, *see Thomas*, 2013 WL 6000484, at *4-6. *See also United States v. Dodson*, 960 F. Supp. 2d 689, 692-93 (W.D. Tex. 2013) (denying a similar motion to suppress).

those IP addresses—and the associated computers and users—that are believed to be engaging in the possession or distribution of child pornography. *Id.*

In order to use CPS products, law enforcement must attend and successfully complete a three-day training course. During the course, law enforcement officers are instructed on how to search for child pornography with P2P file-sharing software using both the manual method and the automated CPS method. The officers are then taught how to compare the results, to demonstrate the reliability of the software. *Id.* If a law enforcement officer completes the course, TLO will allow that officer to use the CPS software in his or her jurisdiction. *Id.*

In late 2011, Detective Gerard Eno of the South Burlington Police Department was investigating child exploitation offenses. The particular focus of his investigation was offenders who were using P2P file-sharing software to exchange child pornography files. *Id.* at *7, 11. Detective Eno, who had completed TLO's training course and was licensed by the company to operate its software in Vermont, used CPS to identify an IP address that had offered to share images and video files that were tagged as being potentially child pornography. Detective Eno confirmed that the files indeed

constituted child pornography by cross-referencing them with other databases and file-share systems.[5] *Id.* at *11.

Using the IP address obtained through CPS, Detective Eno traced the computer to a physical address in Vermont, which turned out to be where defendant Derek Thomas lived. Special App. 41. After conducting a period of surveillance on this residence, a search warrant application for the address was submitted to a magistrate judge. Accompanying the application was a 22-page affidavit by Homeland Security Investigations Special Agent Seth Fiore (the "Fiore Affidavit"), which included a detailed explanation of: (1) P2P file-sharing; (2) how P2P file-sharing software is used to exchange child pornography; (3) the use made, in general, of CPS software during the investigation; and (4) the grounds for probable cause to search the target address and any computers found there (including a description of the files that the CPS software detected on defendant's computer). *Id.* at 56-82. While the Fiore Affidavit described the use of CPS software in general terms, it did not identify the company that created the software, or refer to the software by name. *Id.* at 14-15.

---

[5] Detective Eno did not attempt to directly download the files from the IP address but, instead, relied upon "historical" information to establish that they constituted child pornography. Specifically, Detective Eno compared the hash values—or the "digital fingerprints"—of the defendant's files with the hash values of images known to be child pornography that had previously been downloaded from the Internet by law enforcement. Using this base of comparison, he was able to establish that the defendant's files were child pornography for the purpose of the affidavit. *Thomas*, 2013 WL 6000484, at *3, 7.

The magistrate judge issued the requested search warrant. *Id*. at 42. Law enforcement agents executed a search on the residence and on Thomas's computer. *Id*. at 42-43. Child pornography files were thereafter found on the computer. *Id*. at 43.

Thomas filed four separate motions to suppress the evidence seized pursuant to these searches. Following a consolidated suppression and *Franks* hearing,[6] the District Court denied Thomas's motions, concluding that probable cause existed for the search of Thomas's residence and computer.

Relevant here, the District Court found that the Fiore Affidavit adequately disclosed the fact that law enforcement used automated software in conducting its investigations and that Thomas's challenge to the reliability of the automated software was unsupported by any evidence. The District Court also found that the

[6] It bears recalling that the purpose of a *Franks* hearing is for a defendant to demonstrate that statements in an affidavit intentionally or recklessly misled a district court. In *Franks v. Delaware*, 438 U.S. 154 (1978), the Supreme Court ruled that while a presumption of validity attaches to a law enforcement affidavit, in certain circumstances a defendant is entitled to a hearing in order to test the veracity of an affiant's statements. *Id*. at 171. To suppress evidence obtained pursuant to an affidavit containing erroneous information, a defendant is required to show that: "(1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the issuing judge's probable cause or necessity finding." *United States v. Rajaratnam*, 719 F.3d 139, 146 (2d Cir. 2013) (quoting *United States v. Canfield*, 212 F.3d 713, 717-18 (2d Cir. 2000)) (internal quotation marks and brackets omitted).

primary function of CPS is simply to produce lists of otherwise public information.

DISCUSSION

The question before us is whether, under the totality of the circumstances, the Fiore Affidavit provided a substantial basis for the magistrate judge's conclusion that there was probable cause that child pornography would be found on a computer in Thomas's residence.

The standard of review for evaluating the district court's ruling on a suppression motion is clear error as to the district court's findings of historical facts, but *de novo* as to ultimate legal conclusions, such as the existence of probable cause. *United States v. Raymonda*, 780 F.3d 105, 113 (2d Cir. 2015).

Probable cause "is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Maryland v. Pringle*, 540 U.S. 366, 370-71 (2003) (citation omitted). Indeed, the probable-cause standard is "incapable of precise definition or quantification into percentages because it deals with probabilities and depends on the totality of the circumstances." *Id*. at 371.

When reviewing a challenged warrant, we "accord considerable deference to the probable cause determination of the issuing magistrate." *Walczyk v. Rio*, 496 F.3d 139, 157 (2d Cir. 2007). This degree of deference derives from a concern that "[a] grudging

or negative attitude by reviewing courts toward warrants will tend to discourage police officers from submitting their evidence to a judicial officer before acting." *United States v. Ventresca*, 380 U.S. 102, 108 (1965). Accordingly, the task of a reviewing court is simply to ensure that the totality of the circumstances afforded the magistrate "a substantial basis" for making the requisite probable cause determination. *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

We have previously held that "to suppress evidence obtained pursuant to an affidavit containing erroneous information, the defendant must show that: (1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the issuing judge's probable cause or necessity finding." *United States v. Rajaratnam*, 719 F.3d 139, 146 (2d Cir. 2013) (quoting *United States v. Canfield*, 212 F.3d 713, 717–18 (2d Cir. 2000)) (internal quotation marks and brackets omitted). In the case of omissions, we explained that "the ultimate inquiry is whether, after putting aside erroneous information and correcting material omissions, there remains a residue of independent and lawful information sufficient to support a finding of probable cause or necessity." *Id*. (*quoting Canfield*, 212 F.3d at 718) (internal quotation marks and brackets omitted). In general, it is strong evidence that the Government did not deliberately falsify information in the affidavit, or act with "reckless disregard for the truth," when the alleged omission would have strengthened, rather than weakened, the Government's showing of probable cause. *See id.* at 155.

Here, Thomas asserts that the evidence recovered from his computer must be suppressed because the Government omitted two crucial items of information from the affidavit that the magistrate relied upon in issuing the relevant search warrants: (1) the fact that CPS, a third-party software source, generated the information upon which the Government relied; and (2) information regarding the reliability of the CPS software.[7]

I. Disclosure of CPS in the Affidavit

Thomas asserts that the Fiore Affidavit did not adequately disclose or describe the use of CPS to generate the evidence that the Government relied upon in its warrant application.

Thomas's disclosure claim can be divided into two separate, but related, challenges: (1) that the Fiore Affidavit failed to disclose the third-party nature of CPS, *see* Appellant's Br. 28; and (2) that the Fiore Affidavit failed to disclose the commercial name of CPS, *id.* at 36.

---

[7] Thomas also argues that the warrant, if valid, did not authorize the search of his computer because he was an "unanticipated guest" in the home where the search occurred. This contention is baseless—as the agents confirmed before seizing Thomas's computer, the defendant had been staying at the address listed on the affidavit for 10 months. *See* Gov't App. 13. Nonetheless, defendant advances a novel interpretation of the Fourth Amendment that would require law enforcement to obtain an additional "warrant to search a specific computer device" within an otherwise searchable area. Appellant's Br. 19. For substantially the reasons stated by the District Court, *see* Special App. 43-46, we decline to adopt such a requirement.

Both challenges are without merit. The fact that the software was created by a third-party is immaterial here. The software, as explained below, merely aggregates existing public information, and so its provenance has no bearing on the probable cause determination. Indeed, defendant presents no case law or other authority for his assertion that law enforcement was required to explicitly state the non-governmental nature of the software's creator. In any case, the District Court concluded that the affidavit at issue *did* adequately disclose "the use of third party software to identify the IP address of a target computer and to monitor and log Internet and local network traffic from that IP address." *Thomas*, 2013 WL 6000484, at *8.

In the same vein, Thomas provides no case law or other authority to support his argument that the Government was required to disclose the commercial name of the software used to uncover evidence of his crime. We have never held that the anonymity of a source of information destroys the veracity of an affidavit, especially where the source is known, disclosed, and described, with only its name withheld.[8] Rather, when the Supreme Court, in *Illinois v. Gates*, 462 U.S. at 238, "reaffirm[ed] the totality-of-the-circumstances analysis" for probable cause determinations, it also reaffirmed the value of "anonymous citizen informants" and the need for a "common-sense" approach to assessing the "veracity"

[8] *See, e.g.*, *United States v. Smith*, 9 F.3d 1007, 1013 (2d Cir. 1993) (finding "it [ ] certainly not fatal" when an affidavit is based on an anonymous informant's statements which the Agent "did not personally witness").

and "basis of knowledge" of those informants. *Id.* Requiring the Government to name the third-party software vendor in the affidavit—in addition to the detailed description of the software—would run counter to the general reasoning of *Illinois v. Gates*.

Moreover, just as an informant's name can be presented anonymously in an affidavit, *see id.*, so too can a company's name. Probable cause determinations can hang solely on the *veracity* of an informant, but not on that informant's name. So too, the primary relevance of automating third-party software lies not in its name, but in its *functionality*.[9] And in this case, the functionality of the software—and all of the material facts relating to law enforcement's reliance on it—were clearly described in the affidavit. Specifically, the affidavit disclosed that law enforcement used automated software during the course of this investigation, noted the software's purpose, and then went into considerable detail as to how the software operated. No additional or more specific information was necessary.

Finally, we cannot conclude that any omission here was made deliberately or with "reckless disregard for the truth" when it is clear that full disclosure of the relevant information would only have *strengthened* the search warrant application. *Rajaratnam*, 719 F.3d at 155. In fact, during the proceedings in the District Court,

[9] There may be situations where the Government has reason to believe that facts beyond the software's functionality (*e.g.*, a company's notorious reputation for unreliability) bear on the probable cause analysis. In such a case, not disclosing the company's name in a search warrant affidavit could arguably be considered a material omission relevant to probable cause.

Thomas conceded that if the affidavit had contained more detailed information it would have strengthened, not weakened, the Government's case for probable cause. J.A. 546-47.

II. Reliability of CPS

Thomas also asserts that the affidavit failed to establish the reliability of the CPS software at issue, drawing a parallel to the drug-sniffing dog in *Florida v. Harris*, 133 S. Ct. 1050 (2013). There, the Supreme Court held that a drug-sniffing dog's satisfactory performance in a certification or training program is a sufficient basis to trust his alert and thus establish probable cause. Thomas contends that no such certification or testing was done on the CPS software, thereby calling into question the subsequent probable cause determination generated by law enforcement's use of CPS.

Thomas' reliability challenge fails for several reasons. First, his analogy to a drug-sniffing dog is inapposite. Employing a drug-sniffing dog to establish probable cause involves numerous steps, each of which is susceptible to error: (1) the training of the dog to identify illicit substances; (2) the dog's ability to follow its training in identifying a particular illicit substance; (3) the dog appropriately signaling to law enforcement that an illicit substance is present; and (4) a law enforcement agent's ability to properly interpret that signal. Moreover, any such error along this chain is not always

discernible to law enforcement, as dogs contain certain sensory abilities that are far superior to those of humans.[10]

By contrast, the CPS software merely automates the aggregation of public information—a task that could otherwise be performed manually by law enforcement, albeit at a slower and less efficient pace.[11] Moreover, as the District Court found, the CPS software is built directly on the source code (*i.e.*, the digital skeleton)

---

[10] *See, e.g*, *Florida v. Harris*, 133 S. Ct. at 1056 (noting that law enforcement may not be able to discern whether a canine actually erred if the dog signaled illegality to law enforcement after detecting illegal substances that were well-hidden, present in small quantity, or present only in some residual form).

[11] *See Thomas*, 2013 WL 6000484, at *6 ("[CPS products] are evidence-gathering tools that merely obtain, report, and categorize information regarding files that are available for sharing from a particular IP address. A law enforcement officer must then take further steps to determine whether the information received supports a conclusion that there is probable cause to believe that evidence of child pornography will be found at a particular physical address."); *see also United States v. Naylor*, No. Crim. A. 2:14-194, 2015 WL 730078, at *4 (S.D. W. Va. Feb. 19, 2015) ("[T]he CPS program works by listening over, and performing searches on, Internet networks. In doing so, it attempts to find those users offering, or desiring, results associated with child exploitation."); *United States v. Dennis*, No. 3:13-cr-10-TCB, 2014 WL 1908734, at *2 (N.D. Ga. May 12, 2014) ("[CPS] collects publicly available information."); *Dodson*, 960 F. Supp. 2d at 692 ("To root out purveyors of child pornography on these P2P networks, law enforcement agencies have developed specialized software to troll public networks, identify files containing child pornography, locate the users sharing these files, and catalog all of this public information. One example of this type of software is the Child Protection System (CPS).").

of the file-sharing programs and so, unlike a sniffing dog, the risk of error, if any, is drastically reduced.[12]

A hypothetical question is illuminating—would the probable cause calculus be different if a police officer witnessed a drug deal or if a pre-positioned CCTV camera was able to capture that same transaction? Clearly not. Similarly, the probable cause calculus should be the same here, regardless of whether the CPS software detected Thomas's sharing of child pornography by automatically collecting and assessing public traffic over a P2P network, or whether Detective Eno witnessed the sharing of those same illicit files on a P2P network in real time.

In any case, we discern no error—much less, clear error—in the District Court's finding that CPS was a reliable tool that could serve as the basis of a search warrant affidavit.[13] The District Court found that there was no evidence "that CPS products report false or misleading information," nor was there any evidence presented demonstrating that CPS was not reliable. *Thomas*, 2013 WL 6000484, at *6. Finally, the District Court also found that there are no

---

[12] The District Court concluded that, because CPS is based upon the same protocol used by the file-sharing network, it is not clear what, if any, adjustments could be made to render the software more reliable. *See Thomas*, 2013 WL 6000484, at *6.

[13] *See also*, *e.g.*, *Naylor*, 2015 WL 730078, at *5 ("The CPS software appears to be a reliable investigative tool for law enforcement in [child pornography] cases.").

industry-accepted tests or methodology that could have been used to further enhance the reliability of CPS software.[14] *Id.*

Based upon an examination of the totality of the circumstances, there existed sufficient "indicia of reliability" to permit a reasonable person to conclude that probable cause existed in these circumstances. *Illinois v. Gates*, 462 U.S at 233. Law enforcement verified and corroborated the information received from CPS through a hash-value analysis,[15] and cogently made the case in their affidavit such that a reasonably prudent person, viewing the evidence "through the lens of common sense . . . would . . . think that a search would reveal contraband or evidence of a crime." *Florida v. Harris,* 133 S. Ct. at 1058.

---

[14] An affidavit relying upon CPS software was similarly challenged in an Ohio child pornography case, *Mahan v. Bunting*, No. 1:13-CV-165, 2014 WL 1153444 (N.D. Ohio Feb. 3, 2014), *report and recommendation adopted as modified*, 2014 WL 1154054 (N.D. Ohio Mar. 20, 2014). The *Mahan* Court also held that a warrant predicated on information obtained from automated P2P software was sufficient to establish probable cause. As that court put the point, "[d]efendant has not provided us with a single authority, in Ohio or otherwise, that found suppression was warranted where law enforcement obtained a search warrant based on the use of technology that searches open peer-to-peer networks." 2014 WL 1153444, at *10.

[15] *See supra* n.4 and accompanying text.

CONCLUSION

We hold that probable cause was sufficiently established in the affidavit at issue and that Thomas's motions to suppress were thus properly denied.

For the reasons set forth above, we **AFFIRM** the District Court's March 31, 2014, judgment**.**