# United States Court of Appeals
## FOR THE EIGHTH CIRCUIT

No. 07-3222

| | | |
|---|---|---|
| United States of America, | * | |
| | * | |
| Appellee, | * | |
| | * | Appeal from the United States |
| v. | * | District Court for the |
| | * | District of North Dakota. |
| Steven Bruce Cartier, | * | |
| | * | |
| Appellant. | * | |

Submitted: April 15, 2008
Filed: September 19, 2008

Before MURPHY, COLLOTON, and SHEPHERD, Circuit Judges.

SHEPHERD, Circuit Judge.

Reserving his right to appeal the district court's[1] ruling on his motion to suppress evidence and statements, Steven Cartier entered a conditional plea of guilty to: one count of sexual exploitation of minors in violation of 18 U.S.C. § 2251(a), (e); one count of possession of materials involving sexual exploitation of minors in violation of 18 U.S.C. § 2252(a)(4)(B), (b)(2); one count of making a false, fictitious and fraudulent statement in violation of 18 U.S.C. § 1001(a)(2); and eight counts of receipt of materials involving the sexual exploitation of minors in violation of 18

[1]The Honorable Rodney S. Webb, United States District Judge for the District of North Dakota.

U.S.C. § 2252(a)(2), (b)(1). Cartier challenges the denial of his motion to suppress. We affirm.

I.

Using the information obtained from the Spanish Guardia Civil Computer Crime Unit ("SGCCCU"),[2] the Federal Bureau of Investigation ("FBI") obtained a search warrant for Cartier's home. The information was obtained during the course of an SGCCCU investigation involving a peer-to-peer ("P2P") file sharing network. Working in conjunction with a private company, the SGCCCU has developed a search engine to conduct searches of P2P networks using the "hash values" of files shared by people using the network. Every digital image or file has a hash value, which is a string of numbers and letters that serves to identify the image or file.[3] P2P networks allow computers to share files with each other without using a central file server. Instead, every computer connected to the P2P network can send and receive files because each computer acts as both a server and a client. Therefore, each computer that is logged into the P2P network can share information and obtain information from any other computer that is part of the P2P network. P2P networks are often used in the unauthorized exchange of copyrighted music files. Likewise, P2P networks are commonly used to exchange images involving child pornography.

[2]The SGCCCU is the computer crimes division of the Spanish Civil Guard, a Spanish national law enforcement agency.

[3]In this case, the "hash values" were unique sets of 32 numbers and letters that were calculated using a mathematical algorithm that considered certain data contained in individual files.

In the course of its investigation, the SGCCCU collected several images depicting child pornography previously seized by law enforcement.[4] The SGCCCU then logged the hash value numbers for each digital image and made the images available on the Edonkey P2P network, which is a file sharing network used to exchange digital images. Using the logged hash values, the SGCCCU kept track of which computer internet service provider ("ISP") addresses downloaded the digital images known to be child pornography.

After documenting that several of the digital images known to be child pornography were downloaded by an ISP address associated with a computer in North Dakota, the SGCCCU notified the FBI's Innocent Images Unit ("IIU"). The case was then assigned to Special Agent Christopher Boeckers. Agent Boeckers eventually determined that the ISP address belonged to Cartier and the computer corresponding to that address was located in Cartier's home.

Using the information obtained from the SGCCCU, the FBI obtained a search warrant for Cartier's home. Cartier was not present when the agents went to his home to serve the search warrant, so they went to his place of employment. After advising Cartier that they were going to execute the search warrant, the agents gave Cartier the opportunity to return to his home in order to open the door to his residence rather than the door being broken down in order for the agents to gain entry. After Cartier opened the door for the agents, he was directed first to a squad car and then to his own living room. Once inside his living room, Cartier was told that he was not under arrest, he was not required to talk to the officers, and he was free to leave. After being so advised, Cartier agreed to speak to the agents.

[4]These digital images consisted of pornographic photos of children less than 10 years of age engaged in sexual acts.

During the interview, Cartier admitted that he used a P2P file sharing network and had previously downloaded child pornography from other similar file sharing networks. He acknowledged that some of the images depicted children from one to five years of age. He also told the agents that some of his child pornography files involved scenarios such as rape, but he denied that he ever engaged in sexual activity with a child. The agents then asked Cartier for permission to see his work computer. At that time, the agents followed Cartier back to his place of employment and confiscated his work computer.

During the execution of the search warrant, agents seized and searched 13 hard drives, two thumb drives and hundreds of compact discs and video tapes. Over 1,000,000 still images of child pornography and more than 4,000 video images of child pornography were found on the computer seized from Cartier's residence. One of the video files depicted Cartier engaging in sexual activity with a prepubescent female.

Cartier was arrested May 9, 2006, and a criminal complaint was filed on the same day. Cartier's initial appearance was conducted the following day. On June 7, 2006, a grand jury indicted Cartier, and a superceding indictment was filed on April 12, 2007. After his motion to suppress evidence and statements was denied, Cartier entered a conditional plea of guilty to all counts of the superceding indictment. He now appeals the denial of his suppression motion.

II.

On appeal, Cartier argues that the district court erred in denying his motion to suppress because (1) the agent failed to establish that there was probable cause to issue the search warrant, (2) the search warrant was overly broad and did not articulate a search strategy, and (3) he was not advised of the Miranda warnings prior to giving his statement.

III.

When we review a district court's denial of a motion to suppress, we review its factual findings for clear error and its legal findings de novo. United States v. Engler, 521 F.3d 965, 969 (8th Cir. 2008).

Cartier asserts that probable cause was lacking for issuance of the search warrant because (1) Agent Boeckers's affidavit relied upon the hash values of digital files which had not been viewed prior to the issuance of the search warrant, (2) no person had seen images of child pornography on Cartier's computer prior to the execution of the search warrant, (3) the information relied upon was from a source whose credibility as a reliable law enforcement agency had not been established, and (4) the search warrant affidavit did not contain a search date by the SGCCCU that would assure the information was not stale. "Probable cause exists when a 'practical, common-sense' inquiry that considers the totality of the circumstances set forth in the information before the issuing judge yields a 'fair probability that contraband or evidence of a crime will be found in a particular place.'" United States v. Stevens, 530 F.3d 714, 718 (8th Cir. 2008) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

In arguing that the hash values do not establish probable cause for a search warrant, Cartier asserts that it is possible for two digital files to have hash values that collide or overlap. The district court heard the factual evidence presented on the issue of hash values at the suppression hearing. Cartier's expert testified that hash values could collide and that in laboratory settings these values had done just that. However, the government's expert witness testified that no two dissimilar files will have the same hash value. After hearing all of the evidence presented by both parties, the district court settled the factual dispute about hash values in favor of the view offered by the government. After reviewing the transcript of the suppression hearing, we do not find that the trial court clearly erred in making the factual finding with respect to hash values.

Although Cartier correctly asserts that no one reported seeing images of child pornography on his computer prior to the execution of the search warrant, the lack of such evidence does not necessitate a finding that probable cause was lacking. Indeed, search warrants are issued based on the totality of the circumstances indicating that it is fairly probable, not certain, that the contraband will be found at the place to be searched. See id.

Cartier also argues that, because Agent Boeckers had not verified the reliability of the SGCCCU prior to the issuance of the search warrant, the search warrant was lacking in probable cause. However, the district court heard evidence establishing that, although Agent Boeckers had no personal knowledge of the workings of the SGCCCU, the FBI as an agency considered the SGCCCU to be a reliable law enforcement agency that used a trustworthy means of computer forensics. Testimony was presented at the suppression hearing as to the FBI's agency determination that the SGCCCU was a professional and reliable police agency which had previously provided reliable information to law enforcement agencies in other countries on numerous occasions. Agent Boeckers testified that he believed the SGCCCU to be a reliable police agency in Spain at the time the search warrant was issued for Cartier's home. He also testified that the FBI's IIU was familiar with the SGCCCU and the IIU was his source of information about the SGCCCU. Boeckers testified that FBI field agents routinely rely on information provided to them by the IIU, and in turn the IIU relies on information provided by the SGCCCU. We do not find that the district court erred in its determination that the SGCCCU was a reliable source upon which the issuing judicial officer relied.

Cartier argues that the search warrant affidavit lacked any reference to when the SGCCCU determined that Cartier's computer contained files with hash values matching known child pornography files, and therefore, the issuing judge was unable to determine if the information was stale at the time the search warrant was issued.

Cartier does not allege that the information was actually stale, only that the affidavit did not contain information that would allow the issuing judge to determine if it was stale. Despite Cartier's claims otherwise, the search warrant affidavit clearly states that the SGCCCU matched the hash values on October 22 and 23, 2005, and that on December 27, 2005, the North Dakota Telephone Company, in response to Department of Justice/FBI Administrative Subpoena, confirmed that the ISP address belonged to Cartier on those dates and provided a physical address for Cartier. Thus, Cartier's argument is without merit.

Cartier next asserts that the search warrant was overbroad because it lacked a specific search strategy for the search of his 13 computers and the files they contained. "The Fourth Amendment requires a showing of probable cause before a search warrant may be issued." United States v. Williams, 477 F.3d 554, 557 (8th Cir. 2007). Prohibiting the issuance of general search warrants, the Fourth Amendment requires that a search warrant describe and identify the items to be seized with particularity. United States v. Nieman, 520 F.3d 834, 839 (8th Cir. 2008). Cartier does not assert that the search warrant failed to describe and identify the items to be seized from his computer; instead he argues that the absence of a search strategy renders a search warrant invalid per se. Although this issue has not previously been decided in this circuit, this argument has been rejected in other circuits. See United. States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1108 (9th Cir. 2008) (while a warrant may arguably provide for a less invasive search, the requirement of a pinpoint search limited to an e-mail program or specific search terms is not likely to cast a net sufficiently wide to capture the evidence sought by the search warrant); United States v. Khanani, 502 F.3d 1281, 1290 (11th Cir. 2007) (absence of written search protocol did not render the search warrant overbroad); United States v. Hill, 459 F.3d 966, 977-978 (9th Cir. 2006) (defendant's proposed search methodology is unreasonable and overlooks the probability that perpetrators will attempt to save files using names not obviously associated with the crimes at issue); United States v. Brooks, 427 F.3d 1246, 1251-52 (10th Cir. 2005) (the warrant need not include a search protocol to

satisfy the particularity requirement of the Fourth Amendment and defendant failed to suggest how the search would have been different with a scripted search protocol).

Cartier argues that the search warrant should have had a search strategy so that the private files which had no connection to child pornography would not have been included in the search. However, Cartier does not allege that he was prejudiced by any search of unrelated files nor does he allege that any unrelated files were actually searched. The standard used to gauge the particularity requirement of a search warrant is one of "'practical accuracy' rather than a hypertechnical one." United States v. Summage, 481 F.3d 1075, 1079 (8th Cir. 2007), cert. denied, 128 S. Ct. 875 2008) (quoting United States v. Peters, 92 F.3d 768, 769 (8th Cir. 1996)). While we acknowledge that there may be times that a search methodology or strategy may be useful or necessary, we decline to make a blanket finding that the absence of a search methodology or strategy renders a search warrant invalid per se. Therefore, on the facts of this case, we do not find that the absence of a search methodology or strategy was fatal to the validity of the search warrant.

Finally, Cartier argues that his motion to suppress evidence should have been granted as to his statements to law enforcement officers because he was not advised of his rights prior to making his statement pursuant to Miranda v. Arizona, 384 U.S. 436 (1966). "Miranda warnings are required only where a person's freedom has been so restricted as to render him 'in custody.'" United States v. Martinez, 462 F.3d 903, 908 (8th Cir. 2006), cert. denied, 127 S. Ct. 1502 (2007) (quoting United States v. LeBrun, 363 F.3d 715, 720 (8th Cir. 2004)).

The relevant question here is whether Cartier was in custody at the time he made the statement. We review a district court's findings concerning custody for purposes of Miranda for clear error. United States v. J.H.H., 22 F.3d 821, 831 (8th Cir. 1994). In assessing whether Cartier was "in custody" for Miranda purposes, we make a two-part inquiry: (1) was he formally placed under arrest or (2) was his

freedom of movement restrained to the degree associated with a formal arrest. Id. A review of the transcript indicates that Cartier drove his own vehicle from his place of employment to his home in order to facilitate entrance of the officers to his residence. Prior to making his statement, Cartier was advised by FBI agents that he was not required to give a statement and that he was free to leave. When Cartier made his statement, he was in his own living room. After giving his statement, Cartier left his home and drove his own vehicle back to his place of employment in order to give his work computer to the agents. Furthermore, the totality of the circumstances establishes that Cartier's freedom was not restrained as if he were formally under arrest, and he had no reasonable basis to feel that he was so restrained. See United States v. Czichray, 378 F.3d 822, 826 (8th Cir. 2004). Therefore, we do not find that the district court committed clear error in determining that Cartier was not in custody at the time he made his statement.

IV.

For the foregoing reasons, we affirm Cartier's conviction.

---