

contacted on March 1, March 8, and April 10 of 2007 by a person using the AOL screen name "FarlowMeCasa," who made sexual advances on "Chris" and proposed meeting in person for a sexual encounter. Among other statements, "FarlowMeCasa" told "Chris" that he thought Chris would enjoy performing oral sex on him. In one or more of these communications, "FarlowMeCasa" transmitted a non-pornographic, digital image of a bodybuilder and claimed it was a photograph of himself. (First Aff. of Det. Laurie Northrup ¶ III.2, Doc. No. 35-2.) Det. Badalucco informed Det. Northrup that sending written sexual solicitations to an undercover police officer posing as a minor violates the New York crimes of disseminating indecent material to minors in the first degree, New York Penal Law § 235.22, and endangering the welfare of a child, Id. § 260.10 (2009). (Id. ¶ III.4.) Det. Badalucco also informed Det. Northrup that he had already subpoenaed the AOL subscriber information for the "FarlowMeCasa" profile and that AOL had indicated that the profile was registered to Gary Farlow of Litchfield, Maine. (Id. ¶ 3.) Det. Badalucco requested Det. Northrup's assistance in obtaining a search warrant to examine Farlow's computer and related storage devices for evidence of these New York crimes. (Id. ¶ 5.) After an investigation into the location of the Farlow residence, Det. Northrup prepared her affidavit in support of a search warrant application presented to a Maine District Court Judge. Northrup related the information obtained from Det. Badalucco in her affidavit and stated her conclusion that there was probable cause to believe the Farlow residence contained computers and related equipment that were used as instrumentalities in, and that contain evidence of the commission of, the crimes of endangering the welfare of a child and dissemination of indecent material to minors, in violation of New York law. (Id. ¶ V.1.) She represented, among other things, that careful forensic examination would result in the recovery of data to prove these

crimes and represented that the data to be recovered included "graphic visual images." (Id. ¶ V.5.)

The District Court Judge issued a warrant authorizing officers to enter the Farlow residence and seize and search computers and related devices found there for the following:

1. Computers and computer equipment (such as monitors, keyboards, compact disk drives, zip disk drives, USB drives, digital cameras, MP3 players, etc.), electronic data storage devices (such as hard drives, floppy disks, zip disks, compact disks, digital video disks, memory sticks, flash memory cards, etc.), software, and written materials relating to the operation of the computer (such as names of online accounts, screen names, passwords, manuals, computer reference books, guides and notes).

2. Computer records or data, whether in printed or electronic form, that are evidence of the crimes of dissemination of indecent materials to minors or endangering the welfare of a child, including but not limited to records of Internet use (such as Internet browser history, search engine history, temporary Internet files, etc.), electronic communications (such as email and email attachments, records or data pertaining to online chat room communications, file transfer logs, text messages, writings created on word processing software or notepads, etc.), stored data files and folders, graphic visual images (such as photographs, movie clips and scanned images), software or programs for file sharing or peer-to-peer networks, personal calendars or diaries, and any records or data that demonstrate the identity of the person(s) who exercised dominion or control over the computer or its contents.

(Apr. 23, 2007, Search Warrant, Part II, Doc. No. 35-2.)

Det. Northrup executed the search warrant in the afternoon of April 23, 2007. At the time of execution, Det. Badalucco was chatting online with "FarlowMeCasa" in his guise as "Chris" and Detectives Northrup and Badalucco were communicating directly via cell phone. Defendant Gary Farlow was the only person at home at the time of execution and he acknowledged that his AOL screen name was "FarlowMeCasa" and that he had been chatting with "Chris" at the time of Det. Northrup's arrival. (Second Aff. of Det. Northrup ¶ III.7, Gov't Response Ex. B, sealed paper file.) Det. Northrup removed Farlow's computer from the

premises for off-site examination. The following day, Sergeant Glenn Lang of the Maine State Police Computer Crimes Unit conducted a "quick preliminary search" of Farlow's computer by using a program capable of displaying digital images residing on the hard drive of a computer so that he could visually scan the images to locate the body builder image associated with Det. Badalucco's investigation. (Id. ¶ III.8.) Among the digital images that appeared on the screen were several images depicting pre-pubescent children engaged in sexual acts. (Id.) Based on this discovery, Sgt. Lang and Det. Northrup applied for a new search warrant to authorize seizure of the computer and the contraband images. (Id.) The Maine District Court Judge issued the second warrant based on the new probable cause presentation, which including sample images of child pornography. (Apr. 25, 2007, Search Warrant, Gov't Response Ex. B, sealed paper file.)

Sgt. Lang is the Supervisor and Commander within the State Police Computer Crimes Unit for Internet Crimes against Children. He is trained and certified as an Encase Examiner and has been involved in hundreds of electronic forensic examinations. (Decl. of Sgt. Glenn Lang ¶¶ 1-6, Doc. No. 35-4.) Sgt. Lang attests that a search for evidence consisting of a digital image is most pragmatically and efficiently performed visually by placing all digital image files in gallery view and scanning the images by eye to locate copies of the particular image that is sought. (Id. ¶¶ 10-15.) In the case of the search for the body builder image, Sgt. Lang relates that this approach revealed over 130 copies of the image on the hard drive of Farlow's computer with a range of different file names, hash values, file extensions, and locations. (Id. ¶ 16.) He further declares that a more pinpointed search for a file based on file name, hash value, file extension, or likely folder location can all be frustrated by owner manipulation or automatic computer processes. (Id. ¶¶ 10-15.) Although a pinpointed search for the body builder image could have been performed, a visual search is simple and uncovers the most copies of the image, regardless

of the variables associated with file name, hash value, file extension, and likely folder location. In Sgt. Lang's words: "The only reasonable way for an examiner to locate most of the copies of a particular image is to do it visually. . . . This is exactly what was done in the Gary Farlow case and the results [over 130 copies of the body builder image found]. . . demonstrate the need to follow this procedure." (Id. ¶ 15.)

The United States indicted Farlow on March 11, 2009, on child pornography charges. On August 4, 2009, Farlow moved to suppress the images on which the indictment is premised. He requests a hearing in order to establish certain facts that are already evident: that the body builder image is not pornographic, that not every copy of the body builder image needed to be found in order to advance Det. Badalucco's New York investigation, and that a more focused search could have been performed that would have uncovered the body builder image attached to the communications associated with Badalucco's investigation. (Def.'s Reply Mem. at 3, Doc. No. 40.) For example, Farlow observes that Det. Badalucco's investigation already provided forensic examiners with the times and dates of the communications, the addresses involved, and independent copies of the body builder image sent to "Chris." (Def.'s Mot. to Suppress at 3-4, Doc. No. 29.) Such evidence, in Farlow's view, would support a finding that the initial search warrant was unconstitutionally overbroad or was executed in an unlawful manner, and that the second search warrant must also be declared invalid because it was based on illegally obtained evidence acquired pursuant to the first warrant. (Id. at 1-2, 7-8.)

DISCUSSION

"The Fourth Amendment prohibits the issuance of any warrant except one 'particularly describing the place to be searched, and the persons or things to be seized.'" United States v. Rogers, 521 F.3d 5, 9 (1st Cir. 2008) (quoting U.S. Const. amend. IV). "Any search intruding

upon [an individual's] privacy interest must be justified by probable cause and must satisfy the particularity requirement, which limits the scope and intensity of the search." United States v. Bonner, 808 F.2d 864, 867 (1st Cir. 1986). Probable cause to issue a search warrant exists when "given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). "A search warrant application must demonstrate probable cause to believe that: 1) a crime has been committed, and 2) 'enumerated evidence of the offense will be found at the place to be searched[.]'" United States v. Hicks, 575 F.3d 130, 136 (1st Cir. 2009) (quoting United States v. Feliz, 182 F.3d 82, 86 (1st Cir. 1999)). An issuing judge's determination of probable cause deserves "great deference" from reviewing courts. Gates, 462 U.S. at 236. The duty of a court reviewing a decision to issue a warrant is to ensure that the issuing judge had a substantial basis for concluding that probable cause existed. Gates, 462 U.S. at 238-39. In connection with this review, affidavits are "to be interpreted in a common-sense rather than hypothetical or hypertechnical manner." United States v. Garcia, 983 F.2d 1160, 1167 (1st Cir. 1993). Due to the strong preference for warrants under the Fourth Amendment, in a doubtful or marginal case a reviewing court "normally" will defer to the issuing judge's finding of probable cause. United States v. McMullin, 568 F.3d 1, 6 (1st Cir. 2009).

As to particularity, there are two concerns: "one is whether the warrant supplies enough information to guide and control the agent's judgment in selecting what to take, and the other is whether the category as specified is too broad in the sense that it includes items that should not be seized." United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (citations omitted).

In requiring a particular description of articles to be seized, the Fourth Amendment "makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." United States v. Fuccillo, 808 F.2d 173, 175 (1st Cir. 1987) (quoting Stanford v. Texas, 379 U.S. 476, 485 (1965)). Unfettered discretion by the executing officer is one of the principal evils against which the Fourth Amendment provides protection, and thus warrants which lack particularity are prohibited.

United States v. Morris, 977 F.2d 677, 681 (1st Cir. 1992). However, although a warrant cannot contain a "general order to explore and rummage, . . . the degree of specificity required is flexible and will vary depending on the crime involved and the types of items sought." United States v. Greene, 250 F.3d 471, 477 (6th Cir. 2001) (citations and quotation marks omitted).

It cannot be said that the initial warrant that enabled law enforcement to acquire Farlow's computer was imprecise or overly broad in authorizing a search that extended to data stored on Farlow's computer. Authorization of a search of the computer was particular to the computer crime at issue. When the affidavit's recitation of probable cause describes the kind of computer crime at issue in this case, specification that a computer's contents will be searched is reasonably precise. For one thing: "A search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs." Upham, 168 F.3d at 535. Moreover: "As a general proposition, any container situated within residential premises which are the subject of a validly-issued warrant may be searched if it is reasonable to believe that the container could conceal items of the kind portrayed in the warrant." United States v. Gray, 814 F.2d 49, 51 (1st Cir. 1987) (citing United States v. Ross, 456 U.S. 798, 820-21 (1982)). See also Rogers, 521 F.3d at 9-10 (holding that warrant authorizing a search for "photos" reasonably authorized a search for images that might be found on a videotape). The warrant's authorization to retain Farlow's computer for purposes of a forensic examination was

not overbroad because the probable cause recited by Det. Northrup was particularized with respect to computer crime.

Fowler argues that the initial warrant was nevertheless overbroad because it did not impose a search protocol that would prevent an examination designed to reveal digital images stored on his computer irrespective of file name, file location, or other restrictions. He also maintains that Sgt. Lang did not reasonably tailor his search to focus on the crimes under investigation. (Mot. to Suppress at 6-8.)

The response of the United States is somewhat overstated with respect to its position that the investigation depended upon a search that would return the greatest number of copies of the body builder file or in regard to its position that "[a] more limited search parameter was not possible." (Gov't Response at 1, 11, Doc. No. 35.) However, it acknowledges that the search authorized by the warrant "did not permit . . . a wholesale or blanket seizure [search] of all records without any reference to the crime under investigation." (Id. at 7.) Authorization was necessarily limited, says the United States, to "evidence of dissemination of indecent materials to minors or endangering the welfare of a child." (Id.) In this regard, the United States argues that Sgt. Lang was entitled to visually scan images on the computer as one practical and efficient approach to finding evidence of the body builder image that Farlow attached to his communications with "Chris." (Id. at 10.)

I conclude that the probable cause recited in the warrant would have supported an explicit authorization to conduct a software-enabled visual scan of images located on the hard drive as one reasonable means of tracking down the body builder image (and related communications), because that image was evidence of the criminal conduct under investigation, even though it was not itself contraband. There is no need for a hearing to support a finding that Sgt. Lang could

have focused his investigation on the AOL chat room communications, which may have or would have turned up evidence of the body builder image directly co-located with the pertinent criminal communications data. There is no constitutional requirement that investigators must conduct a search in any particular sequence in order to minimize the likelihood of uncovering contraband or other evidence of a crime, and the imposition of a search protocol ruling out a visual image search in a case like this would only afford special protection to those who engage in criminal conduct by computer. See Upham, 168 F.3d at 537 ("The . . . warrant did not prescribe methods of recovery or tests to be performed, but warrants rarely do so. The warrant process is primarily concerned with identifying what may be searched or seized—not how—and whether there is sufficient cause for the invasion of privacy thus entailed."); see also United States v. Cameron, ___ F. Supp. 2d ___, No. 09-CR-24-B-W, 2009 U.S. Dist. Lexis 79684, *10-13, 2009 WL 2832247, *4 (D. Me. Sept. 1, 2009). Farlow's use of the body builder image opened the door to an image search because such a search is not unreasonable given the legitimacy of searching for the body builder image as evidence of the crimes under investigation. That the ensuing discovery of child pornography may have been anticipated or other than inadvertent does not change this analysis. Horton v. California, 496 U.S. 128, 138-40 (1990).

This case is entirely unlike United States v. Carey, 172 F.3d 1268 (10th Cir. 1999), where officers perused image files on a computer as part of a search for documentary evidence of the sale and distribution of controlled substances. Additionally, unlike the case of United States v. Otero, 563 F.3d 1127 (10th Cir. 2009), relied upon by Farlow, extending the warrant's authorization to search for digital images did not result in a general warrant because Farlow's use of the body builder image creates a nexus between an image file search and the crimes for which probable cause to search existed. That nexus was also spelled out in the instant search warrant,

which authorized a search of computer records or data "that are evidence of the crimes of dissemination of indecent materials to minors or endangering the welfare of a child," unlike the warrant at issue in Otero, which did not limit the computer search/seizure to specific crimes as it did with respect to other items taken from the defendant's home. Id. at 1132-33. This case is more like United States v. Giberson, 527 F.3d 882 (9th Cir. 2008), where the Court upheld a search using "ILOOK" software that, like the Encase software, enabled investigating officers to display image files in a gallery view for efficient visual inspection on a warrant that authorized a search for images associated with the production of false identification cards, leading to discovery of child pornography. Id. at 889-890.

Imposing a search protocol to restrict a computer search is something that a judge may do in an appropriate case. However, I cannot say that the state judge's failure to impose a search protocol prohibiting a visual scan of image files resulted in an overbroad warrant or that Sgt. Lang's adoption of such an approach went beyond the scope of the warrant's authorization to seize or search for image files. Given the evidentiary value of the body builder image, this is not a case where the absence of a prohibition against a gallery review of image files, or the use of such a search strategy, triggers a Fourth Amendment violation. Consequently, I conclude that no Fourth Amendment violation is associated with the computer search pursuant to the first warrant. Because the officers in this case quite appropriately sought a second warrant when the visual scan revealed images of child pornography, I also reject the contention that evidence seized pursuant to the second warrant must be suppressed.

CONCLUSION

For the reasons set forth above, I RECOMMEND that the Court DENY Defendant's Motion to Suppress (Doc. No. 29).

NOTICE

A party may file objections to those specified portions of a magistrate judge's report or proposed findings or recommended decisions entered pursuant to 28 U.S.C. 636(b)(1)(B) for which *de novo* review by the district court is sought, together with a supporting memorandum, and request for oral argument before the district judge, if any is sought, within ten (10) days of being served with a copy thereof. A responsive memorandum and any request for oral argument before the district judge shall be filed within ten (10) days after the filing of the objection.

Failure to file a timely objection shall constitute a waiver of the right to *de novo* review by the district court and to appeal the district court's order.

/s/ Margaret J. Kravchuk
U.S. Magistrate Judge

September 29, 2009

Case title: USA v. FARLOW

Date Filed: 03/11/2009

Assigned to: JUDGE JOHN A.
WOODCOCK, JR

Defendant (1)

GARY A FARLOW

represented by **VIRGINIA G. VILLA**
FEDERAL DEFENDER'S OFFICE
KEY PLAZA, 2ND FLOOR
SUITE 206
23 WATER STREET
BANGOR , ME 04401
(207) 992-4111 Ext. 102
Email: Virginia_Villa@fd.org
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
*Designation: Public Defender or
Community Defender Appointment*

Pending Counts

UNLAWFUL
TRANSPORTATION OF CHILD
PORNOGRAPHY, 18:2252A(a)(1),
2252A(b)(1) and 2256(8)(A)
(1-11)

UNLAWFUL POSSESSION OF
CHILD PORNOGRAPHY,
18:2252A(a)(5)(B), 2252A(b)(2)
and 2256(8)(A)
(12)

Highest Offense Level (Opening)

Felony

Terminated Counts

None

**Highest Offense Level
(Terminated)**

None

Complaints

None

Plaintiff

USA

Disposition

Disposition

Disposition

represented by **JAMES M. MOORE**
OFFICE OF THE U.S. ATTORNEY
DISTRICT OF MAINE
202 HARLOW STREET, ROOM
111
BANGOR , ME 04401
945-0344
Email: jim.moore@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED