United States Court of Appeals
For the First Circuit

No. 11-1975

UNITED STATES OF AMERICA,

Appellee,

v.

GARY FARLOW,

Defendant, Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

[Hon. John A. Woodcock, Jr., U.S. District Judge]

Before

Torruella, Boudin, and Thompson,
Circuit Judges.

Virginia G. Villa, Assistant Federal Defender, for appellant.
Margaret D. McGaughey, Appellate Chief, with whom Thomas E. Delahanty, II, United States Attorney, was on brief, for appellee.

June 1, 2012

THOMPSON, Circuit Judge. After a district judge denied Gary Farlow's motion to suppress the fruits of an allegedly illegal search of his home computer, Farlow pled guilty to one count of Unlawful Transportation of Child Pornography, 18 U.S.C. § 2252A(a)(1). His guilty plea was conditioned on his ability to bring this appeal broadly challenging the denial of his motion to suppress. Farlow's appeal raises some interesting arguments, but in the end they cannot carry the day: for the reasons that follow, we affirm the denial of his motion to suppress, and his conviction therefore stands.

From February through April 2007, a person using the AOL screen name "FarlowMeCasa" contacted a putative 14-year-old AOL user who was actually Detective Peter Badalucco, a member of New York's Nassau County Police Department. FarlowMeCasa sent several explicit messages to Badalucco, including proposals to meet in person for sex; Badalucco believed these messages constituted the crimes of disseminating indecent materials to minors in the first degree (N.Y. Penal Law § 235.22) and endangering the welfare of a child (N.Y. Penal Law § 260.10). Also, on March 8 FarlowMeCasa sent Badalucco an image of a bodybuilder, saying it was an image of himself; this act, though apparently not criminal, will be relevant later.

While FarlowMeCasa was sending these messages, Badalucco was looking into the person behind the screen name. He subpoenaed AOL

for FarlowMeCasa's subscriber information, and AOL informed him that the account belonged to Gary Farlow of Litchfield, Maine. On April 13, Badalucco contacted Maine-based Detective Laurie Northrup to obtain and execute a search warrant of Farlow's residence. Northrup determined that a Gary Farlow, born in 1945, indeed resided in Litchfield, Maine. She also determined that Farlow had been convicted of public lewdness in 1974, disorderly conduct in 1997 (a crime that had originally been charged as indecent conduct), and indecent conduct in 2002.

Based on Farlow's criminal history and his alleged attempts to solicit sex from Badalucco (who, again, had presented himself as a 14-year-old), Northrup prepared an application for a search warrant. A Maine state judge signed off on the warrant, authorizing police to search Farlow's home for the following:

> 1) Computers and computer equipment (such as monitors, keyboards, compact disk [sic] 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 [sic], digital video disks [sic], 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.

The warrant specified that "all of" this material "constitute[s] evidence of the" New-York-state crimes noted above.

On April 23, 2007, the Maine State Police executed the search warrant, appearing at Farlow's home while he was chatting online with Badalucco. The police seized Farlow's computer and "other electronic equipment." A police search of the computer using a forensic program to open image files in a gallery view[1] turned up some child pornography. The police sought and obtained a second warrant geared specifically toward this new discovery; a subsequent search yielded 3,366 images of child pornography, 95 emails sent from the computer with child pornography attachments, and 54 emails received with child pornography attachments. These images and emails led to Farlow's March 11, 2009 federal-court indictment on twelve child-pornography-related charges.

On August 4, 2009, Farlow moved to suppress the fruits of the search authorized by the first warrant (including the second warrant). He argued that the first warrant facially authorized an

[1] In a gallery view, small or "thumbnail" versions of the images appear on-screen, allowing the viewer to browse many images quickly and efficiently.

essentially unfettered search of his computer and therefore failed the Fourth Amendment's probable-cause and particularity requirements. Additionally, he argued, the actual search of his computer could not be saved by various exceptions to the warrant requirement, and even if the warrant had been valid the search had still exceeded the scope of its authorization. Finally, he requested an evidentiary hearing to explore the propriety of the warrant and search. The government responded that the warrant was in fact limited "to computers, computer equipment and computer records or data that are evidence of two specific crimes." Further, the government argued, the search itself "complied, as it must, with the terms of the warrant." In any event, it said, "images of child pornography unavoidably came within [the searching officer's] plain view" during a reasonable search for the bodybuilder image and were therefore exempted from the warrant requirement. And because both the warrant and the search were plainly legal, it said, there was no need for a hearing.

A magistrate judge tasked with reviewing Farlow's suppression motion penned a report and recommendation suggesting that the district court deny the motion. The magistrate judge determined that the warrant was founded on probable cause, it was sufficiently particular, it authorized the search as conducted, no hearing was necessary, and suppression was not appropriate. In a separate

written opinion dated December 3, 2009, a district judge adopted and affirmed the magistrate judge's recommendation in full.

After several continuances, on November 9, 2010 Farlow entered a guilty plea on one count of the indictment, conditioned on his right to appeal the denial of his suppression motion. Following one more false start (Farlow moved to withdraw his plea; the motion was denied), Farlow was sentenced to ten years in prison followed by supervised release for life.

Farlow now appeals, arguing that we must suppress the evidence of child pornography because: (1) the warrant allowed a search that was overbroad given the narrow scope of the government's probable cause; (2) the computer search unlawfully exceeded even the broad scope of the warrant; (3) the plain-view and good-faith exceptions to the warrant requirement do not apply; and (4) even if we disagree with him on the first three issues, we should nevertheless remand for a hearing on the validity of the warrant and search. The government responds (among other things) that there was probable cause to believe Farlow had committed New-York-state indecency crimes, the warrant was tailored to allow police to search for evidence of those crimes, and the police reasonably executed such a search to produce that evidence given the ease of disguising computer files. In reviewing the denial of Farlow's suppression motion, we apply clear-error review to any factual disputes and consider legal issues de novo, United States v.

Materas, 483 F.3d 27, 32 (1st Cir. 2007); we review the denial of an evidentiary hearing for abuse of discretion, United States v. Mitchell-Hunter, 663 F.3d 45, 53 (1st Cir. 2011).

We begin with Farlow's argument that the first warrant was not supported by probable cause. "Probable cause 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." United States v. Crespo-Ríos, 645 F.3d 37, 42 (1st Cir. 2011) (alteration in original) (internal quotation marks omitted). Farlow claims that "the Government had no probable cause to collect any electronic image other than the single nonpornographic image of a bodybuilder." The government responds that Farlow's focus on the bodybuilder image is too myopic: "Farlow's proposal that [Badalucco] meet him in person for sex" and "his prior convictions for . . . deviant behavior" provided probable cause for a much broader search.

We agree with the government: the affidavits submitted in support of the warrant established a fair probability that Farlow's computer and other digital devices held much more evidence than just the bodybuilder image. Most notably, Farlow could have saved transcripts or screenshots of his sexual-solicitation chats with Badalucco, and these could have been stored on any form of digital media -- CDs, DVDs, flash drives, disconnected hard drives, and so on. Probable cause therefore supported a warrant authorizing

police to search broadly for evidence directly related to Farlow's New York crimes, and the warrant here did just that. For essentially the same reason -- the likelihood that police would find evidence in different forms and on different devices, all explicitly listed in the warrant -- the warrant was particular enough to pass constitutional muster. See United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (to be sufficiently particular, a warrant must supply information about what may be seized and must not include items that cannot be seized).

That leaves the question whether the police stayed within the warrant's bounds when executing the search. Farlow says no: the police could (and should) have employed a limited search only for the bodybuilder image, using the image's "hash value" -- a sort of digital fingerprint tied not only to a specific file but also to that file's precise location on a computer.[2] Farlow says that, had the police conducted only a hash-value search instead of a gallery-view search, they likely would have found the bodybuilder image but would not have turned up child pornography. For this reason, he concludes, the search was too invasive and the district court should have suppressed the child-pornography evidence.

---

[2] More specifically, a file's hash value is a short, unique set of numbers and letters produced by running the complex strings of data that make up a computer file through a mathematical algorithm. See Ty E. Howard, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, 19 Berkeley Tech. L.J. 1227, 1233-34 (2004).

The problem for Farlow is that we have rejected the idea that government agents should so narrowly restrict their searches of digital devices. "When searching digital media for 'chats' and other evidence of enticement" -- like the bodybuilder image -- "government agents cannot simply search certain folders or types of files for keywords." Crespo-Ríos, 645 F.3d at 43 (emphasis added). The same goes for other specific identifying information -- like hash values. This is because computer files are highly manipulable. Id. at 43-44. A file can be mislabeled; its extension (a sort of suffix indicating the type of file) can be changed; it can actually be converted to a different filetype (just as a chat transcript can be captured as an image file, so can an image be inserted into a word-processing file and saved as such). See id. Any of these manipulations could change a document's hash value. And in any event a limited hash-value search would not have turned up any chat transcripts (which, again, can be saved as image files) or other evidence of Farlow's New York crimes.[3] The government therefore reasonably executed a broad search that fell within the scope authorized by the valid warrant it obtained.

[3] Farlow argues in his reply brief that the broad search in Crespo-Ríos was justified by the defendant's "statements indicating there may [have been] evidence of other victims on the computer," and that there are no similar statements here. But this argument reflects Farlow's too-narrow focus on the bodybuilder image as the sole source of probable cause. Here, a sweep of image files could reasonably have turned up evidence beyond the bodybuilder image -- like chat transcripts -- and was therefore justified.

Because the warrant and search were valid here, suppression is not warranted. And because that conclusion renders irrelevant the reason for Farlow's requested evidentiary hearing -- to assess the propriety of the police's eschewing a hash-value search -- we affirm the district court's denial of such a hearing. United States v. Panitz, 907 F.2d 1267, 1273-74 (1st Cir. 1990) (holding that a district court does not abuse its discretion by denying an evidentiary hearing in a criminal case where no material facts are in dispute). The end result: we affirm the district court in full, and Farlow's conviction stands. **So ordered.**