In the
United States Court of Appeals
For the Seventh Circuit

No. 11-3716

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

RONALD A. SEIVER,

Defendant-Appellant.

Appeal from the United States District Court
for the Central District of Illinois.
No. 4:10-cr-40091-JES-JAG-1—**James E. Shadid**, *Chief Judge*.

ARGUED AUGUST 7, 2012—DECIDED AUGUST 28, 2012

Before POSNER, TINDER, and HAMILTON, *Circuit Judges*.

POSNER, *Circuit Judge*. The defendant pleaded guilty to possession of child pornography and sexual exploitation of a child, see 18 U.S.C. §§ 2252A(a)(5)(B), 2251(a), and was sentenced to 420 months in prison. But he reserved the right to appeal for the limited purpose of challenging the legality of the search that had yielded evidence that substantiated his guilt. The appeal presents the recurrent issue of "staleness" as a

basis for concluding that a computer search warrant was not supported by probable cause.

The warrant affidavit said that law enforcement authorities had discovered that a pornographic video which a 13-year-girl had made of herself and uploaded to the Internet had been downloaded to a computer at the defendant's home and that 16 still images from that video—three of which were pornographic images of the girl—had been uploaded from that computer to an image-sharing website. A Facebook message with a link to that website had been sent to the girl's stepmother from the same computer. She alerted the authorities, who identified the computer's Internet Protocol address from the website. The address was registered to Ronald Seiver, the defendant.

He argues that there was no reason to believe that seven months after he had uploaded child pornography there would still be evidence of the crime on his computer. Actually a search of his computer was likely to find evidence of three crimes: receipt of child pornography (the downloading of the pornographic video); distribution (the uploading of the pornographic images he obtained from the video); and possession (the storage of the pornography on his computer). 18 U.S.C. §§ 2252, 2252A. He was allowed to plead guilty to only the last of these crimes (besides the sexual-exploitation offense, which was unrelated to the video), though there is no doubt that he committed the other offenses as well. Even if he had deleted the child pornography, a successful recovery of the images from his hard

drive by an FBI computer forensic expert would establish that he had possessed them at one time, well within the five-year statute of limitations.

Nevertheless he contends that the facts that would establish probable cause for a search of his computer were "stale." He adds that downloading a single video and uploading still images derived from it could not establish that he was a "collector" of child pornography who could therefore be assumed to retain indefinitely any illegal pornographic images that he had downloaded. The government concedes the premise that "stale" computer contents are not a permissible basis for a determination of probable cause but argues that a law enforcement officer "could reasonably have concluded that the [defendant], like the vast majority of those who possess and distribute child pornography, would still be in possession of those photographs months later"—that he was, in other words, a "collector."

So the parties agree on the framework for analysis—the importance of "staleness" and the importance to a determination of "staleness" of whether the suspect was a "collector" and thus likely to have "retained" or "maintained" rather than "destroyed" the pornographic images that he had acquired. The parties are faithfully reciting terms appearing in a *very* large number of cases concerning probable cause for a computer search. See, e.g., *United States v. Pappas*, 592 F.3d 799, 803-04 (7th Cir. 2010); *United States v. Prideaux-Wentz*, 543 F.3d 954, 958-59 (7th Cir. 2008); *United States v. Estey*, 595 F.3d 836, 839-40 (8th Cir. 2010); *United States v. Lemon*,

590 F.3d 612, 614-16 (8th Cir. 2010); *United States v. Potts*, 586 F.3d 823, 830 (10th Cir. 2009); *United States v. Paull*, 551 F.3d 516, 522-23 (6th Cir. 2009); *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008); *United States v. Perrine*, 518 F.3d 1196, 1205-06 (10th Cir. 2008); *United States v. Irving*, 452 F.3d 110, 125 (2d Cir. 2006). But the parties to this case, and the authors of the opinions in the cases we've just cited (and in other cases that we could cite involving computer searches for child pornography), appear to be laboring under the misapprehension that deleting a computer file destroys it, so that if the defendant had deleted the pornographic images between their uploading to the Internet and the search of his computer the search would not have yielded up the images, or evidence of their earlier presence in the computer, unless it's a case in which the defendant is a "collector" of child pornography who decided to "keep" copies of the images that he'd downloaded.

The concern with "staleness" versus freshness and "collecting" versus destroying reflects a misunderstanding of computer technology. (A number of cases, however, though none in our court, reflect the correct understanding. See, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).) When you delete a file, it goes into a "trash" folder, and when you direct the computer to "empty" the trash folder the contents of the folder, including the deleted file, disappear. But the file hasn't left the computer. The trash folder is a waste-

paper basket; it has no drainage pipe to the outside. The file *seems* to have vanished only because the computer has removed it from the user interface and so the user can't "see" it any more. Virginia M. Kendall & T. Markus Funk, *Child Exploitation and Trafficking* 275-76 (2012); *United States v. Flyer*, 633 F.3d 911, 918 (9th Cir. 2011); *United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir. 2006) (en banc). But it's still there, and normally is recoverable by computer experts until it's overwritten because there is no longer unused space in the computer's hard drive.

How soon a file will be overwritten depends on a number of factors: whether the user is computer savvy and has installed a program that accelerates the normal overwriting of deleted data, how often he saves new files to his hard drive, the capacity of the hard drive, and how the computer's file system allocates new files. But we know that the FBI routinely extracts incriminating deleted files from hard drives, usually without difficulty. See, e.g., FBI, "Occupational Technology—Overview," www.fbi.gov/about-us/otd/overview (all websites visited Aug. 15, 2012); U.S. Dep't of Justice, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement" 16, 21, 39 (April 2004), www.ncjrs.gov/pdffiles1/nij/199408.pdf; John Patzakis, "Computer Forensics as an Integral Component of the Information Security Enterprise" 3 (Guidance Software 2003), http://faculty.usfsp. edu/gkearns/Articles_Fraud/computerforensics.pdf; Wade Davies, "Computer Forensics: How to Obtain and Analyze Electronic Evidence" *The Champion*, June 2003, p. 34, www.nacdl.org/Champion.aspx?id=807.

And since a deleted file is not overwritten all at once, it may be possible to reconstruct it from the bits of data composing it (called "slack data"), which are still retrievable because they have not yet been overwritten even if overwriting has begun. Before a file is deleted, the file system marks it as unavailable to be overwritten. Once it is deleted, its data are no longer protected against being overwritten, but the file system won't necessarily overwrite it all at once, and if it's only partially overwritten computer experts can recover the portion of the data that has not been overwritten, or at least can match it to images they obtained from (as in this case) a website, to verify that the images were once in the computer's hard drive and thus had been possessed. See Michele C.S. Lange & Kristin M. Nimsger, *Electronic Evidence and Discovery: What Every Lawyer Should Know Now* 235 (2d ed. 2009). Although a savvy computer user can as we said direct his computer to ensure quick (even instantaneous) overwriting, the default settings on standard operating systems don't do this.

"Staleness" is highly relevant to the legality of a search for a perishable or consumable object, like cocaine, but rarely relevant when it is a computer file. Computers and computer equipment are "not the type of evidence that rapidly dissipates or degrades." *United States v. Vosburgh*, 602 F.3d 512, 529 (3d Cir. 2010). Because of overwriting, it is *possible* that the deleted file will no longer be recoverable from the computer's hard drive. And it is also *possible* that the computer will have been sold or physically destroyed. And the longer the interval between the uploading of the material sought as evidence and the search of the computer, the greater

these possibilities. But rarely will they be *so* probable as to destroy probable cause to believe that a search of the computer will turn up the evidence sought; for probable cause is far short of certainty—it "requires only a probability or substantial chance of criminal activity, not an actual showing of such activity," *Illinois v. Gates*, 462 U.S. 213, 244 n. 13 (1983), and not a probability that exceeds 50 percent ("more likely than not"), either. *Hanson v. Dane County*, 608 F.3d 335, 338 (7th Cir. 2010). Notice too that even if the computer is sold, if the buyer can be found the file will still be on the computer's hard drive and therefore recoverable, unless it's been overwritten. The search warrant will have designated the premises where the computer was expected to be found, and though a computer sold by the occupant will obviously no longer be there, evidence may be found there of the buyer's identity.

Computer procedures such as "defragmenting," "wiping," and creating "garbage files" can make deleted computer files very difficult or even impossible to recover. Lange & Nimsger, *supra*, at 221-24. And encryption may hide files remaining on the hard drive so effectively as to thwart their recovery by computer experts. Kendall & Funk, *supra*, at 167. Software that wipes the hard drive or overwrites deleted files with garbage data can be bought on line. But it appears that few consumers of child pornography (the producers may be more savvy) understand well enough how their computer's file system works to grasp the importance of wiping or overwriting their deleted pornographic files or encrypting them securely if they want to avoid leaving recoverable

evidence of child pornography in their computer after they've deleted it. Anyway this way of thwarting a search has nothing to do with staleness. A child pornographer who wants to render computer files nonrecoverable will first download those he wants to keep to a DVD, which can be hidden outside his home, and then either destroy the computer and get a new, "clean" one, or take steps to assure the complete overwriting of the contents of his hard drive. Nevertheless, despite the availability of software for obliterating or concealing incriminating computer files, the use of such software "is surprisingly rare." Kendall & Funk, *supra*, at 276.

No doubt after a *very* long time, the likelihood that the defendant still has the computer, and if he does that the file hasn't been overwritten, or if he's sold it that the current owner can be identified, drops to a level at which probable cause to search the suspect's home for the computer can no longer be established. But seven months is too short a period to reduce the probability that a computer search will be fruitful to a level at which probable cause has evaporated.

Some cases, illustrated by *United States v. Allen*, *supra*, 625 F.3d at 843, say it's important that the search warrant affidavit apprise the magistrate asked to issue the warrant that deleted files are recoverable. That may be prudent, because some magistrates may not know a great deal about computers, but it shouldn't be required to make the warrant valid; it is or should be common knowledge.

Now it is true that after deleting a file and emptying the trash bin containing it, a computer owner who is not

technologically sophisticated no longer "possesses" the file in a meaningful sense, see, e.g., *United States v. Moreland*, 665 F.3d 137, 152 (5th Cir. 2011), and the crime of which the defendant was committed requires knowing possession. Had the defendant deleted the incriminating files (and emptied his trash folder with those files in it), he would no longer have knowingly possessed them if, as in *Moreland*, he could no longer access them because he lacked the software that he would have needed to be able to recover them from the hard drive's slack space. *United States v. Flyer*, *supra*, 633 F.3d at 918-20. But this need not have eliminated probable cause for a search of his computer unless the statute of limitations on possession had expired by the time the search was conducted, which it had not done in this case. See *United States v. Kain*, 589 F.3d 945, 948-50 (8th Cir. 2009).

The most important thing to keep in mind for future cases is the need to ground inquiries into "staleness" and "collectors" in a realistic understanding of modern computer technology and the usual behavior of its users. Only in the exceptional case should a warrant to search a computer for child pornography be denied on either of those grounds (there are of course other grounds for denial). But future changes in computer technology may alter this conclusion, and judges as well as law enforcers must be alert to that possibility as well.

AFFIRMED.
