FOR PUBLICATION

UNITED STATES COURT OF APPEALS
THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee,* v. ANDREW EDWARD FLYER, *Defendant-Appellant.*	No. 08-10580 D.C. No. 4:05-CR-01049-FRZ-GEE OPINION

Appeal from the United States District Court
for the District of Arizona
Frank R. Zapata, District Judge, Presiding

Argued and Submitted
April 15, 2010—San Francisco, California

Filed February 8, 2011

Before: Andrew J. Kleinfeld, A. Wallace Tashima, and
Sidney R. Thomas, Circuit Judges.

Opinion by Judge Thomas

COUNSEL

Nina Wilder; Weinberg & Wilder; San Francisco, California, for the appellant.

Dennis K. Burke, United States Attorney, District of Arizona; Christina M. Cabanillas, Appellate Chief for United States Attorney; and Celeste Benita Corlett, Assistant United States Attorney, Tucson, Arizona, for the appellee.

OPINION

THOMAS, Circuit Judge:

Andrew Flyer appeals his conviction in federal district court under 18 U.S.C. § 2252 (2004) for two counts of attempted transportation and shipping of child pornography (Counts One and Two); one count of possession of child pornography on the unallocated space of a Gateway computer hard drive (Count Three); and one count of possession of child pornography on CDs (Count Four). Flyer contends that the evidence was insufficient to establish the jurisdictional and intent elements of his convictions on Counts One and Two and the possession element of his conviction on Count Three.[1] We agree and reverse in part.

[1]Because we reverse Flyer's Count Three conviction, we decline to reach Flyer's challenge to the district court's denial of his motion to dismiss either Count Three or Count Four on the basis of multiplicity. We also decline to reach Flyer's insufficient-evidence challenge to the jurisdictional element of Count Four, as Flyer conceded the issue at oral argument.

I

A. Preliminary Investigation and Execution of Search Warrant

On March 9, 2004, FBI Special Agent Robin Andrews, acting undercover from Tucson, Arizona, allegedly initiated a session on LimeWire, a peer-to-peer file sharing program. LimeWire and similar programs connect network participants directly and allow them to download files from one another. *See Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 919-20 (2005). To download a file, a LimeWire user opens the application and inputs a search term. LimeWire then displays a list of files that match the search terms and that are available for download from other LimeWire users. When a user downloads a file using the LimeWire network, he or she causes a digital copy of a file on another user's computer to be transferred to his or her own computer. *See Arista Records LLC v. Lime Group LLC*, 715 F. Supp. 2d 481, 494 (S.D.N.Y. 2010).

Andrews launched LimeWire and typed in the search term "PTHC," an apparent acronym for "pre-teen hardcore," a term associated with child pornography. She identified a file titled "O-KIDDY-PTHC BW025.jpeg" and selected a host computer that appeared to have the file available for download. Andrews then clicked "browse host," a LimeWire feature that allows users to view all the files available for download from a host computer's "share" folder. The host computer Andrews had selected listed 261 files available for download, including around twenty files with titles associated with child pornography. Andrews downloaded "O-KIDDY-PTHC BW025.jpeg" from the host computer. She tried to download a second file from the same host, but was unsuccessful.

On March 10, 2004, Andrews allegedly again used LimeWire to search the term "PTHC" and determined that the same host computer had sixty files available for download

with titles associated with child pornography. Andrews downloaded one file containing such a title, and tried, but was again unable, to download a second file from the host computer.

Andrews identified the Tucson, Arizona, residential address associated with the host computer by contacting an internet access provider in Arizona. Flyer lived at the Tucson address, along with his father, mother, and sister.

After securing a warrant, agents executed a search of the property on April 13, 2004. They seized from Flyer's bedroom a Gateway computer, loose media (CDs, floppy disks, and DVDs), and an Apple laptop. They also seized a thumb drive and a family computer that did not contain any child pornography.

Agents interviewed Flyer, who admitted, according to Andrews's testimony, that he used the Gateway computer and Apple laptop in his bedroom, that he had downloaded, saved, and shared child pornography through LimeWire, and that he knew it was illegal to possess child pornography. Flyer also admitted to having saved a minimal amount of child pornography onto his shared folder on LimeWire and around one hundred child pornography files on a computer.

B. Forensic Examination of Electronic Devices

1. The Apple Laptop

FBI Special Agent Steven Gumtow examined Flyer's Apple laptop. He determined that LimeWire had been installed on the laptop and that the setup required the laptop user to manually activate LimeWire each time the laptop was turned on. When a user runs LimeWire, all files on the user's computer located in folders designated as "shared" folders are made available for upload to other LimeWire users. Gumtow testified that the settings on Flyer's laptop were customized to

cap the maximum number of uploads at one file at a time by up to twenty individuals. Defense computer forensics expert Tami Loehrs, on the other hand, testified that the upload bandwidth setting on the laptop was set to zero, which allows only a small amount of data to be leaked out.

The directories set up for sharing on the laptop through LimeWire included the directory "Z" and its folder "R@Y," two directories where Flyer had admitted to saving child pornography. In a subfolder of "R@Y," Gumtow discovered files identical to those that Andrews claimed to have downloaded.

Before Gumtow performed his analysis, the Apple laptop had been in the custody of FBI Special Agent Robert J. Meshinsky. While attempting to image the laptop's hard drive, Meshinsky mistakenly allowed his own computer's operating system to mount on the laptop and access the files stored there. He later testified that he noticed the problem approximately one hour after he had booted up the laptop. He stopped the process, researched another method to use, and successfully copied the hard drive. In his report, Meshinsky made no mention of the improper mounting of the target hard drive. He stated that "[a]pproved procedures and protocols were used as tested and verified by the FBI," a statement which he later admitted to be false.

Defense expert Loehrs independently examined the Apple laptop and discovered that 6,100 files listed last access dates of November 3, 2005, when Meshinksy examined the machine, and that an additional 63,000 files—including the two files allegedly downloaded by Andrews on March 9 and 10, 2004—listed last access dates of March 18, 2005, between 2:05 p.m. and 3:53 p.m. Both dates post-dated seizure of the laptop from Flyer's residence. No information could be recovered regarding any previous access dates for the two files. Meshinsky reviewed Loehrs's findings and agreed with them.

2. The Gateway Computer

FBI Special Agent Christopher Pahl examined the hard drive from the Gateway computer. After duplicating the hard drive to preserve the evidence, Pahl searched the duplicate drive using the term "r@ygold," which is associated with child pornography. The search produced numerous positive hits all over the drive, but the only images believed to be child pornography and later listed in the indictment were found in "unallocated space."

3. The Loose Storage Media.

FBI Analyst Tammy Lepisto examined the CDs, DVDs, and floppy disks seized from Flyer's bedroom. Lepisto determined that twenty-six CDs contained images believed to be child pornography. One file Lepisto located on Flyer's CDs was titled "r@ygold style ST 06122.jpeg." That file, among others, was later listed under Count Four of the indictment.

C. Indictment

A superceding indictment filed in January 2006 charged Flyer with two counts of attempted transportation and shipping of child pornography— specifically, the images allegedly downloaded by Andrews on March 9 and 10, 2004—in violation of 18 U.S.C. §§ 2252(a)(1) and (b)(1) (Counts One and Two); possession of child pornography on the Gateway computer on or about April 13, 2004, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (Count Three); and possession of child pornography on CDs, in violation of § 2252(a)(4)(B) and (b)(2) (Count Four).[2] The jury returned guilty verdicts on all four counts, and the district court sentenced Flyer to concurrent terms of 60 months imprisonment.

[2]A fifth count for possession of child pornography on the Apple laptop was later voluntarily dismissed by the government.

II

[1] Flyer contends that the district court erred when it denied his motion to dismiss Counts One and Two on due process grounds and to suppress evidence pursuant to *United States v. Loud Hawk*, 628 F.2d 1139, 1152 (9th Cir. 1979) (en banc) (Kennedy, J., concurring), *overruled on other grounds by United States v. W.R. Grace*, 526 F.3d 499, 505-06 (9th Cir. 2008) (en banc), based on the FBI's mishandling of his Apple laptop.

We review de novo a due process claim involving the government's failure to preserve potentially exculpatory evidence. *United States v. Cooper*, 983 F.2d 928, 931 (9th Cir. 1993). We review factual findings, such as the absence of bad faith, for clear error. *United States v. Hernandez*, 109 F.3d 1450, 1454 (9th Cir. 1997); *United States v. Booker*, 952 F.2d 247, 249 (9th Cir. 1991).

[2] The government's failure to preserve potentially exculpatory evidence rises to the level of a due process violation if a defendant can show that the government acted in bad faith. *Arizona v. Youngblood*, 488 U.S. 51, 58 (1988). Bad faith requires more than mere negligence or recklessness. *Id.* If the government destroys evidence under circumstances that do not violate a defendant's constitutional rights, the court may still impose sanctions including suppression of secondary evidence. *Loud Hawk*, 628 F.2d at 1152 (Kennedy, J., concurring). In so doing, the court must balance "the quality of the Government's conduct and the degree of prejudice to the accused." *Id.* "The Government bears the burden of justifying its conduct and the defendant bears the burden of demonstrating prejudice." *Id.*

[3] Here, the district court did not clearly err in finding no evidence of bad faith. The government presented evidence that Meshinsky did not intentionally corrupt data on the Apple laptop hard drive, but rather mishandled it. The government

also voluntarily dismissed the count in the indictment relating to possession of child pornography on the Apple laptop. We thus affirm the district court's denial of Flyer's motion to dismiss Counts One and Two on the basis of a due process violation.

[4] The district court properly denied Flyer's request for suppression of the evidence. First, as we explained above, there is no clear error in the district court's determination that the government's conduct evidenced negligence, rather than bad faith. On the other side of the scale, Flyer did not show that mishandling of the evidence prejudiced his defense. That the government could no longer prove the success of the downloads does not prove that Andrews never downloaded the files or that properly preserved data on the Apple laptop would have exculpated Flyer. Indeed, Andrews's testimony indicates that Flyer admitted to using LimeWire to download child pornography on his laptop. We thus affirm the district court's denial of the suppression motion.

III

[5] Flyer next argues that the district court erred in denying his motion for a *Franks* hearing[3] and for suppression of the evidence derived from the April 13, 2004, search based on false and intentionally misleading statements in the affidavit supporting the search warrant. We review Flyer's challenge de novo, *see United States v. Gonzalez, Inc.*, 412 F.3d 1102, 1110 (9th Cir. 2005), and affirm.

When requesting a *Franks* hearing based on allegations of material false statements or omissions in an affidavit supporting a search warrant, a defendant must make a " 'substantial preliminary showing' " that false or misleading statements were (1) deliberately or recklessly included in an affidavit submitted in support of a search warrant; and (2) " 'necessary

[3]*See Franks v. Delaware*, 438 U.S. 154 (1978).

to the finding of probable cause.' " *United States v. Craighead*, 539 F.3d 1073, 1080 (9th Cir. 2008) (quoting *Franks*, 438 U.S. at 155-56).

[6] Flyer did not make a substantial preliminary showing that Andrews lied when she claimed in the affidavit to have downloaded two images of child pornography from Flyer's computer. As the district court determined, evidence of corruption of data on the Apple laptop does not indicate that Andrews lied before the computer was seized.

[7] Andrews's statements concerning her inability to download additional files due to traffic on Flyer's laptop similarly fail to justify a *Franks* hearing. We agree with the district court that these statements were not necessary to the finding of probable cause. The district court properly denied Flyer's motion for a *Franks* hearing.

[8] As Flyer did not demonstrate the invalidity of the search warrant, his motion to suppress evidence derived from the April 13, 2004, search also fails.

IV

Flyer challenges the sufficiency of the evidence to support his conviction. When a sufficiency-of-the-evidence claim is properly preserved, "review of the constitutional sufficiency of evidence to support a criminal conviction is governed by *Jackson v. Virginia* . . . ." *United States v. Nevils*, 598 F.3d 1158, 1163 (9th Cir. 2010) (citing *Jackson v. Virginia*, 443 U.S. 307, 319 (1979)). *Jackson* establishes a "two-step inquiry." *Id.* at 1164. "First, a reviewing court must consider the evidence presented at trial in the light most favorable to the prosecution." *Id.* "Second, . . . the reviewing court must determine whether this evidence, so viewed, is adequate to allow any rational trier of fact [to find] the essential elements of the crime beyond a reasonable doubt." *Id.* When a sufficiency-of-the-evidence claim is not properly preserved, we apply plain-

error review. *See United States v. Cruz*, 554 F.3d 840, 844 (9th Cir. 2009). "Under plain-error review, reversal is permitted only when there is (1) error that is (2) plain, (3) affects substantial rights, and (4) seriously affects the fairness, integrity, or public reputation of judicial proceedings." *Id.* at 845 (quotation omitted).

However, plain-error review of a sufficiency-of-the-evidence claim is only "theoretically more stringent" than the standard for a preserved claim. *Id.* at 844; *see also United States v. Garcia-Guizar*, 160 F.3d 511, 517 (9th Cir. 1998) (noting that even under plain-error review, a court should not "affirm a conviction . . . if the record clearly showed that the evidence was insufficient"). "When a conviction is predicated on insufficient evidence, the last two prongs of the [plain-error] test will necessarily be satisfied." *Cruz*, 554 F.3d at 845 (citations omitted).

[9] Here, Flyer did not renew his motion for judgment of acquittal at the close of the evidence and thus did not preserve his claim. Accordingly, we apply plain-error review as described in *Cruz*.

[10] Applying plain-error review, we must vacate Flyer's convictions on Counts One and Two of the superceding indictment pursuant to *United States v. Wright*, ___ F.3d ___, 2010 WL 4345670 (9th Cir. 2010). In *Wright*, we held that 18 U.S.C. § 2252A(a)(1)[4] required actual transportation of child pornography across state lines, *id.* at ___ F.3d ___, *3-*6, and that "a defendant's mere connection to the Internet does not

[4]The jurisdictional element in that statute is effectively identical to that under which Flyer was charged in Counts One and Two of the indictment. *Compare* 18 U.S.C. § 2252A(a)(1) (2003) ("knowingly mails, or transports or ships in interstate or foreign commerce by any means, including by computer, any child pornography") *with id.* at § 2252(a)(1) (2004) ("knowingly transports or ships in interstate or foreign commerce by any means including by computer or mails, any visual depiction" of child pornography).

satisfy the jurisdictional requirement where there is undisputed evidence that the files in question never crossed state lines," *id.* at ___, *6. *Wright*'s holding controls. Here, the government concedes that it presented no evidence at trial directly showing that the two files downloaded by Andrews traveled across state lines. Furthermore, Flyer cites uncontroverted expert testimony that a file shared between two users through LimeWire would not leave Tucson if, as here, both the host computer and recipient were located within that city. Andrews' *intra*state download of files from Flyer's computer cannot by itself, consistent with *Wright,* provide sufficient evidence to convict Flyer of attempting to cause those files' *inter*state or foreign movement. Accordingly, we reverse Flyer's convictions for attempted transportation and shipment of the files in interstate commerce. *See id.* at ___, *12. We thus decline to reach Flyer's additional contention that the requisite specific intent for the crime was not supported by sufficient evidence.

V

[11] Flyer next alleges that the evidence is insufficient to support his conviction on Count Three for possession "on or about April 13, 2004" of child pornography on the Gateway computer in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (2004). Subsection (a)(4)(B) provides that any person who "knowingly possesses . . . with intent to view, 1 or more books, magazines, periodicals, films, videotapes, or other matter" containing visual depictions of a minor engaged in sexually explicit behavior shall be punished as provided in subsection (b)(2). Flyer contends that the evidence is insufficient to establish that he "possesse[d]" the files. We agree.

[12] " 'Possession' is '[t]he fact of having or holding property in one's power; the exercise of dominion over property.' " *United States v. Romm*, 455 F.3d 990, 999 (9th Cir. 2006) (quoting BLACK'S LAW DICTIONARY 1183 (7th ed. 1999)). "[T]o establish possession, the government must

prove a sufficient connection between the defendant and the contraband to support the inference that the defendant exercised dominion and control over [it]." *Id.* (internal quotation omitted) (alteration in the original).

[13] The images charged in Count Three were all located in "unallocated space" on the Gateway hard drive. Unallocated space is space on a hard drive that contains deleted data, usually emptied from the operating system's trash or recycle bin folder, that cannot be seen or accessed by the user without the use of forensic software. Such space is available to be written over to store new information. Even if retrieved, all that can be known about a file in unallocated space (in addition to its contents) is that it once existed on the computer's hard drive. All other attributes—including when the file was created, accessed, or deleted by the user—cannot be recovered.

Files in unallocated space differ from cache files, which are a "set of files kept by a web browser to avoid having to download the same material repeatedly . . . so that the same images can be redisplayed quickly when you go back to them." *Id.* at 993 n.1 (quotation omitted). Cache files are located in "an area to which the internet browser automatically stores data to speed up future visits to the same websites." *Id.* at 994 n.3 (citation omitted). The user does not manually save the cache files, *id.*, but can access them and "print, rename, [or] save [the files] elsewhere, the same thing [he or she could] do with any other file," *id.* at 998 (internal quotation marks omitted).

Flyer argues there was insufficient evidence to establish that he exercised dominion and control over the images recovered from the unallocated space on the hard drive. Alternatively, he argues that even if he could be said to have "possessed" the images before their deletion, no evidence indicated that the possession occurred during the time period charged in the indictment.

Our precedent relating to cache files suggests that a user must have knowledge of and access to the files to exercise dominion and control over them. In *Romm*, we affirmed a defendant's conviction under 18 U.S.C. § 2252A(1)(5)(B) for possession of child pornography images deleted from the internet cache of his computer. *Id.* at 1000. We reasoned that:

> [The defendant] had access to, and control over, the images that were displayed on his screen and saved to his cache. He could copy the images, print them or email them to others, and did, in fact, enlarge several of the images.

Id. at 1001. Moreover, a forensic analysis of the defendant's hard drive indicated that all of the child pornography on his computer (and reflected in his internet history) had been erased after Canada Border Services Agency had seen several pornography websites in the computer's internet history. *Id.* at 994-95.

In comparison, in *United States v. Kuchinksi*, 469 F.3d 853 (9th Cir. 2006), we held that we could not consider images recovered from the cache for purposes of a sentencing calculation when no evidence indicated that the defendant had tried to access the cache files or knew of their existence. *Id.* at 862. We reasoned:

> Where a defendant lacks knowledge about the cache files, and concomitantly lacks access to and control over those files, it is not proper to charge him with possession and control of the child pornography images located in those files, without some other indication of dominion and control over the images. To do so turns abysmal ignorance into knowledge and a less than valetudinarian grasp into dominion and control.

Id. at 863.

The decision of the Court of Appeals for the Armed Forces in *United States v. Navrestad*, 66 M.J. 262 (C.A.A.F. 2008) is in accord. There, the court held that a defendant lacked dominion and control over child pornography images that he viewed while using an internet café computer. *Id.* at 267-68. Although the viewed images had been automatically stored in the computer's temporary cache, the court held that the defendant did not "possess" them. *Id.* The court reasoned that the defendant could not access the hard drive where the cache files had been saved nor download the images to a portable storage device. *Id.* Additionally, no evidence indicated that the defendant had e-mailed or printed copies of the images or that he was aware that he could have done so. *Id.*

[14] We conclude that Flyer's conviction must be reversed under the reasoning in *Romm*, *Kuchinski*, and *Navrestad*. The government concedes that it presented no evidence that Flyer knew of the presence of the files on the unallocated space of his Gateway computer's hard drive. The government also concedes it presented no evidence that Flyer had the forensic software required to see or access the files. Unlike *Romm*, there is no evidence here that Flyer had accessed, enlarged, or manipulated any of the charged images, and he made no admission that he had viewed the charged images on or near the time alleged in the indictment.

The government counters that evidence demonstrating that the files had at some point been deleted, resulting in their placement in unallocated space, is sufficient to establish possession. In support, the government cites *United States v. Shiver*, 305 F. App'x 640 (11th Cir. 2008) (unpublished), for the proposition that one method for a defendant to exercise dominion and control over an image is to destroy a copy of the image located on his computer. *See id.* at 643.[5]

[5]As we recognized in *Romm*, "removal of files from the recycle bin generally requires manual steps to be taken by the user." 455 F.3d at 993 n.2.

[15] But deletion of an image alone does not support a conviction for knowing possession of child pornography on or about a certain date within the meaning of § 2252(a)(4)(B) (2004). No evidence indicated that on or about April 13, 2004, Flyer could recover or view any of the charged images in unallocated space or that he even knew of their presence there. Accordingly, the district court committed plain error, and we reverse Flyer's conviction on Count Three.

VI

[16] We affirm the district court's denial of Flyer's motion for a *Franks* hearing and for suppression of the evidence derived from the April 13, 2004 search. We decline to reverse the convictions on Counts One and Two on the basis of government's failure to preserve potentially exculpatory evidence. We reverse Flyer's convictions on Counts One, Two, and Three. The judgment of the district court is affirmed in part and reversed in part. Because we reverse three of the four counts on which Flyer was convicted and sentenced, we vacate the sentence and remand for resentencing on the remaining count. *See United States v. Avila-Anguiano*, 609 F.3d 1046, 1049 (9th Cir.) (permitting resentencing when part of a multi-count sentence is vacated), *cert. denied*, 131 S. Ct. 586 (2010).

AFFIRMED IN PART; REVERSED IN PART; SENTENCE VACATED and REMANDED.