FILED
United States Court of Appeals
Tenth Circuit

January 5, 2011

Elisabeth A. Shumaker
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

TENTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. TERRY BRIAN DOBBS, Defendant-Appellant.	No. 09-5025

Appeal from the United States District Court
for the Northern District of Oklahoma
(D.C. No. 4:07-CR-00149-GKF-1)

John T. Carlson, Assistant Federal Public Defender (Raymond P. Moore, Federal Public Defender, with him on the briefs), Denver, Colorado, for Defendant-Appellant.

Barak Cohen, Attorney, Criminal Division, United States Department of Justice, Washington, D.C. (Thomas Scott Woodward, Acting United States Attorney, and Leena Alam, Assistant United States Attorney, Tulsa, Oklahoma, on the brief), for Plaintiff-Appellee.

Before **BRISCOE**, Chief Judge, **HOLLOWAY** and **HOLMES**, Circuit Judges.

HOLMES, Circuit Judge.

In this criminal appeal, Terry Brian Dobbs brings a sufficiency-of-the-evidence challenge to his conviction for knowingly receiving and attempting to

receive child pornography in violation of 18 U.S.C. § 2252(a)(2). Mr. Dobbs contends that there was insufficient evidence to prove: (1) that he knowingly received or attempted to receive either of the two pornographic images submitted to the jury; and (2) that these two particular images traveled in interstate or foreign commerce, as required by our precedent in *United States v. Schaefer*, 501 F.3d 1197 (10th Cir. 2007).

Exercising jurisdiction under 28 U.S.C. § 1291, we agree that the government did not offer sufficient evidence to prove that Mr. Dobbs knowingly received the images found on his hard drive. Consequently, because we have no need to opine on the merits of Mr. Dobbs's *Schaefer* argument, we refrain from doing so. We **REVERSE** and remand to the district court to **VACATE** Mr. Dobbs's conviction and sentence.

I. Background

In April 2006, United States Postal Inspectors in Oklahoma seized Mr. Dobbs's computer pursuant to a search warrant issued in an unrelated fraud investigation. A search of the computer revealed multiple images suspected to be child pornography, leading the investigators to obtain a second search warrant. The computer's hard drive was eventually sent to a Department of Justice computer forensic specialist in Washington, D.C. Upon further inspection of Mr.

Dobbs's hard drive, the forensic specialist discovered over 150 images of child pornography in the hard drive's temporary Internet files folder, or "cache."[1]

Mr. Dobbs was subsequently indicted for receipt, attempted receipt, and possession of visual depictions of minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(2) and (a)(4)(B). Prior to trial, the government dismissed the charge of possession in violation of § 2252(a)(4)(B), leaving the single charge that Mr. Dobbs "knowingly received and attempted to receive one or more visual depictions [of minors engaged in sexually explicit conduct], including but not limited to . . . '14[2].jpg' [and] 'b003[1].jpg.'" R., Vol. I, at 109 (Second Superseding Indictment, filed July 11, 2008).

At trial, the government's case relied principally on the testimony of the forensic specialist, who explained in detail the results of his investigation of Mr. Dobbs's hard drive. His analysis indicated both that Mr. Dobbs had typed in multiple search terms reflecting the pursuit of child pornography,[2] and that Mr.

---

[1] The record refers to this folder interchangeably as "temporary internet files folder" and "cache." For consistency and clarity, we refer to it as the cache.

[2] For computers running Microsoft Windows, the Windows registry stores information about the search terms that a user types into Internet search engines. The Windows registry revealed that some of the search terms on Mr. Dobbs's computer included the following: "very young sex," "erotic preteen," "youngest porn," "pedo pics," and "preteen Lolita." R., Vol. III, at 452–56 (Trial Tr., dated Oct. 29, 2008).

Dobbs had visited websites consistent with such pornography.[3] Additionally, the forensic specialist reconstructed some of the pages that resulted from Mr. Dobbs's search activity, noting that after some of the search terms were entered, the user advanced the web browser to get additional results, sometimes up to thirty-six times. He concluded that the computer activity suggested someone who was "methodically seeking out child pornography." R., Vol. III, at 464.

The forensic specialist also testified that the charged photographs recovered from Mr. Dobbs's hard drive were found exclusively in the computer's cache. As he explained it, when a person visits a website, the web browser automatically downloads the images of the web page to the computer's cache. The cache is populated with these images regardless of whether they are displayed on the computer's monitor. In other words, a user does not necessarily have to see an image for it to be captured by the computer's automatic-caching function. Although the forensic specialist noted that a computer user can manipulate some images that appear on a computer's screen, he acknowledged that there was no evidence that Mr. Dobbs actually viewed the charged images, much less clicked on, enlarged, or otherwise exercised actual control over any of them. Furthermore, while the forensic specialist explained that a user may manipulate

[3] Like the Windows Registry and search terms, a computer's "index.dat" file records the websites visited by the computer user. The forensic specialist was able to match up websites listed in the "index.dat" file of Mr. Dobbs's computer with several websites that were consistent with child pornography. *See* R., Vol. III, at 376–77.

and control an image stored in the computer's cache**,** he repeatedly admitted that there was no evidence that Mr. Dobbs had accessed his computer's cache, or that he even knew it existed.

During the trial, the district court initially admitted seventeen images found in Mr. Dobbs's cache. That number was winnowed down to two when the government failed to provide adequate evidence that fifteen of the images had traveled in interstate commerce. The two remaining images—"b003[1].jpg," which was captured by the caching function on Mr. Dobbs's computer on March 15, 2006, at 9:29:56 p.m., and "14[2].jpg," which was captured shortly thereafter at 9:31:17 p.m.—were banner images, comprised of multiple, smaller images, measuring 3.25 inches by .5 inch.[4]

In constructing its case against Mr. Dobbs, the government created a time line of activity aimed at establishing a pattern indicative of the hunt for child pornography. Specifically, the forensic specialist testified that a pattern existed wherein the arrival of suspect images on Mr. Dobbs's computer was immediately preceded by searches using terms typically affiliated with child pornography. However, while such a pattern may have existed for the images ultimately excluded from the jury's consideration, the forensic specialist admitted that there was no evidence of a temporally proximate search indicating the pursuit of child

[4] Officers from the Palm Beach County Sheriff's Office and the Suffolk County Police Department testified that these two banners contained images that were created in Florida and New York.

pornography with respect to the two images submitted to the jury. Nor was he able to present evidence that Mr. Dobbs visited a website typically associated with child pornography immediately preceding the arrival of the two images in his computer's cache.

At the close of the government's case, and again at the close of all the evidence, Mr. Dobbs moved for a judgment of acquittal, arguing that insufficient evidence was presented to prove both the jurisdictional element under *Schaefer* and that he "knowingly" possessed the images found on his hard drive. The district court denied Mr. Dobbs's motions, based in part on its prior ruling limiting the images submitted to the jury. Mr. Dobbs was subsequently found guilty of knowingly receiving and attempting to receive child pornography. The district court sentenced him to 132 months' imprisonment and nine years of supervised release. This timely appeal followed.

II. Discussion

On appeal, Mr. Dobbs argues that we must reverse his conviction because the government offered insufficient evidence to prove that his receipt of child pornography was "knowing," and thus punishable under § 2252(a)(2). More specifically, he claims that the lack of evidence suggesting that he knew of his computer's automatic-caching process forecloses a finding of knowing receipt of the two images submitted to the jury, which were found in the cache. He suggests that "a man who doesn't know he has certain images inside his computer [cannot]

be said to have knowingly accepted those images . . . [or] to have knowingly exercised control over them." Aplt. Reply Br. at 5.

The government, in contrast, contends that Mr. Dobbs's conviction is supportable based in part on evidence that he "engaged in a pattern of methodically seeking out child pornography, by conducting image searches for terms . . . [associated with child pornography] and downloading websites consistent with child pornography." Aplee. Br. at 15–16. This, "combined with the ability [of Mr. Dobbs] to control those images, was sufficient to prove that he received child pornography." *Id.* at 16. In sum, the government argues that "because Dobbs knowingly sought out and accessed the images, and had the ability to control them when they appeared, the statutory definition of receipt was met." *Id.* at 21.

Mr. Dobbs also claims that the government failed to prove the jurisdictional element of the crime, as described in *Schaefer*—namely, that the particular images presented to the jury crossed state lines. *See* 501 F.3d at 1202. Because we find Mr. Dobbs's first argument dispositive, we do not address this second issue.

A. Standard of Review

We review a challenge to the sufficiency of the evidence de novo. *United States v. Vigil*, 523 F.3d 1258, 1262 (10th Cir. 2008). "Evidence is sufficient to support a conviction if, viewing the evidence in the light most favorable to the

government, a reasonable jury could have found the defendant guilty beyond a reasonable doubt." *United States v. LaVallee*, 439 F.3d 670, 697 (10th Cir. 2006) (quoting *United States v. Hien Van Tieu*, 279 F.3d 917, 921 (10th Cir. 2002)) (internal quotation marks omitted). "We will reverse a conviction 'only if no rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.'" *United States v. Willis*, 476 F.3d 1121, 1124 (10th Cir. 2007) (quoting *United States v. Gurule*, 461 F.3d 1238, 1243 (10th Cir. 2006)).

B. Knowing Receipt

Mr. Dobbs was charged with and convicted of knowing receipt and attempted receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2). That statute provides for the punishment of any person who

> knowingly receives . . . any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, . . . if—
>
> > (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
> >
> > (B) such visual depiction is of such conduct . . . .

18 U.S.C. § 2252(a)(2) (2006).[5]

---

[5] Section 2252 has undergone significant amendment since Mr. Dobbs was charged, including a revision that criminalizes knowingly accessing sexually explicit images with the intent to view them. *See* Effective Child Pornography Prosecution Act of 2007, Pub. L. No. 110-358, 122 Stat. 4001, 4002–4003. In this appeal, however, we review the sufficiency of the evidence for Mr. Dobbs's (continued...)

Although "knowingly receives" is not defined in the statute, "in interpreting the term, we are guided by its ordinary, everyday meaning." *United States v. Tucker*, 305 F.3d 1193, 1204 (10th Cir. 2002) (analyzing the term "possesses" under a related statute, 18 U.S.C. § 2252(a)(5)(B)). The district court instructed the jury that to "receive" means "to accept an object and to have the ability to control it." R., Vol. I, at 340 (Jury Instruction No. 16). Neither party has objected to this definition. Consequently, we are comfortable adopting the view that it comports with the word's everyday and ordinary meaning (as appears to be the case). *See* Webster's Ninth New College Dictionary (1985) (defining "receive" as "to come into possession of"); *see also United States v. Stanley*, 896 F.2d 450, 451 (10th Cir. 1990) (approving of the district court's definition of "to receive" under § 2252(a)(2) as "to acquire control, in the sense of physical dominion or apparent legal power to dispose of the [item]").

In addition, the district court instructed the jury that the term "knowingly" means "that an act was done, or visual depictions were received, voluntarily and intentionally, and not because of mistake or accident." R., Vol. I, at 340. We believe that this definition is consistent with the ordinary and everyday meaning of the word as well, and the parties do not argue to the contrary. *See United States v. Fabiano*, 169 F.3d 1299, 1303 (10th Cir. 1999) ("An act is done

---

[5](...continued)
conviction under the law as it existed at the time of the charged offense, not as it stands today.

'knowingly' if done voluntarily and intentionally, and not because of mistake or accident or other innocent reason."); *see also* Tenth Circuit Criminal Pattern Jury Instructions No. 1.37 (2005) ("When the word 'knowingly' is used in these instructions, it means that the act was done voluntarily and intentionally, and not because of mistake or accident.").

There is little doubt that Mr. Dobbs—or at least his computer—"received" child pornography. Indeed, Mr. Dobbs does not contest that the government found images of child pornography on his computer. However, mere receipt of child pornography is not what is proscribed by § 2252(a)(2); rather, it is the *knowing* receipt of this illegal content that is punishable under the statute. *See* 18 U.S.C. § 2252(a)(2).

Mr. Dobbs challenges the sufficiency of the government's evidence establishing that he knowingly received *the two images that were sent to the jury*. A careful review of the record reveals that the government presented no evidence that Mr. Dobbs had accessed the files stored in his computer's cache, including the two images at issue. And, more tellingly, there was no evidence that he even knew about his computer's automatic-caching function. Moreover, as to the two images at issue, there was no evidence presented to the jury that Mr. Dobbs even saw them, much less had the ability to exercise control over them by, for example, clicking on them or enlarging them. As such, although there is no question that a rational jury could have found that Mr. Dobbs "received" the two

images, we conclude that it could not have found that Mr. Dobbs did so *knowingly*.

In resisting such a conclusion, the government relies upon "proof that Dobbs knowingly and methodically sought out child pornography," Aplee. Br. at 19, and posits that the "[f]iles found in Dobbs's [cache] provided circumstantial evidence that he had received images of child pornography, by downloading the websites on which they appeared," *id.* at 16. However, we are not persuaded. The proof that the government relies upon in establishing Mr. Dobbs's intent to seek out child pornography—*viz.*, the pattern of child-pornography-related searches immediately preceding the creation of illegal images in the cache—does not apply to the two images submitted to the jury. The government's own forensic specialist admitted that there is no evidence of suggestive searches immediately prior to the creation of those two images in the cache, nor is there any indication that Mr. Dobbs visited suspect websites prior to their arrival in his cache. The pattern of search-and-creation, therefore, is based solely upon evidence related to the fifteen excluded images, and consequently is irrelevant to the question of whether Mr. Dobbs knowingly received the two images that were properly before the jury.

Furthermore, the government's suggestion that the presence of the child pornography files in the cache of Mr. Dobbs's computer provides circumstantial evidence of knowing receipt is misguided. The mere presence of the files in the

cache is certainly proof that the files were *received* through the automatic-caching process; however, for this evidence to be probative of the question of *knowing* receipt, the government needed to present proof that Mr. Dobbs at least knew of the automatic-caching process. It presented no such proof in this instance.

This proof deficiency is underscored by our decision in *United States v. Bass*, 411 F.3d 1198 (10th Cir. 2005). *Bass* was rendered in an analogous context—a prosecution for possession of child pornography under 18 U.S.C. § 2252A(a)(5)(B). There, a search of the defendant's computer had unearthed over 2000 images of child pornography, although "the origin of the images could not be identified—that is, whether the images had been intentionally or automatically saved to the computer from the internet." *Id.* at 1200. When interviewed by the authorities, the defendant admitted viewing child pornography, but "stated that he did not know (1) how to download images from the internet or (2) that the computer was automatically saving the images he viewed." *Id.* at 1201. Claiming ignorance of his computer's caching function, the defendant argued that his lack of knowledge as to this automatic process should prevent a finding of knowing possession. *Id.* at 1201–02.

Despite the defendant's professed lack of knowledge, we nevertheless affirmed his conviction on appeal. We did so based in large part on evidence that the defendant used software specifically aimed at eliminating the digital residue of his illicit activities, including "History Kill" and "Window Washer." *Id.* at

1202.[6] We concluded that in light of his use of these programs, a "jury . . . reasonably could have inferred that [the defendant] knew child pornography was automatically saved to his mother's computer based on evidence that [he] attempted to remove the images." *Id.*; *see also Tucker*, 305 F.3d at 1204 (finding sufficient evidence to support a conviction of knowing possession of child pornography located in the computer's cache when the defendant admitted that "he knew that when he visited a Web page, the images on the Web page would be sent to his browser cache file and thus saved on his hard drive").

In contrast to *Bass*, the government presented absolutely no evidence here from which a reasonable jury could infer that Mr. Dobbs knew of his computer's automatic-caching function, much less that he had accessed his cache. Consequently, we conclude that the presence of the child pornography files in the cache of Mr. Dobbs's computer does not alone demonstrate—circumstantially or otherwise—his knowing receipt of those files. For us to conclude otherwise would "turn[] abysmal ignorance into knowledge and a less than valetudinarian grasp into dominion and control." *United States v. Kuchinski*, 469 F.3d 853, 863 (9th Cir. 2006).[7]

---

[6] The defendant admitted that he used "History Kill" and "Window Washer" to delete child pornography because "he didn't want his mother to see those images." *Bass*, 411 F.3d at 1202.

[7] The Ninth Circuit's decision in *Kuchinski* also underscores the proof deficiency here. In *Kuchinski*, the court was called on to determine whether

(continued...)

The government vigorously contends that *Bass* and other cases where at least part of the prosecution related to *possession* of child pornography are inapposite because this is "a pure receipt case," where the proof requirements are different. Aplee. Br. at 29. Even assuming *arguendo* that there are significant differences in the proof requirements of possession and receipt prosecutions,[8] the

---

[7](...continued)
images found in the defendant's cache could be used to enhance his sentence for knowingly receiving and possessing child pornography in violation of 18 U.S.C. § 2252A(a)(2) and (a)(5)(B). Although 110 images of child pornography had been found in the defendant's download folders and deleted files folder (recycle bin), more than 1100 illegal images were found in his active cache, and another 13,904 to 17,784 related files were located amongst the deleted temporary Internet files. *Id.* at 856. The district court applied the five-level enhancement that is triggered when over 600 qualifying images are recovered, relying on the additional images found in the computer's cache. *Id.* at 862.

The defendant appealed, claiming that there was insufficient evidence to establish that he knowingly possessed the cached files. The Ninth Circuit, in reviewing the record, agreed that "there was no evidence that Kuchinski was [a] sophisticated [computer user], that he tried to get access to the cache files, or that he even knew of the existence of the cache files." *Id.* at 862. Relying on its earlier decision in *United States v. Romm*, 455 F.3d 990 (9th Cir. 2006), which in turn rested heavily on our decision in *Tucker*, the court concluded that "[w]here 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." *Kuchinski*, 469 F.3d at 863; *see also Romm*, 455 F.3d at 1000 ("[T]o possess the images in the cache, the defendant must, at a minimum, know that the unlawful images are stored on a disk or other tangible material in his possession."). Like *Kuchinski*, there is no evidence in this case that Mr. Dobbs knew of his computer's automatic-caching function or of the files that were created as a result of it.

[8] Although we need not (and do not) definitively opine on the matter, even assuming that different proof standards attend prosecutions for possession
(continued...)

government's arguments are unavailing because they do not square with the language of the receipt statute. The government contends that "in a pure receipt case, evidence that the defendant intentionally sought out child pornography establishes that his receipt was knowing." *Id.* The government, in effect, is positing that defendants need not know that they actually have received child pornography—through automatic caching or otherwise—to be convicted of *knowing* receipt of child pornography, so long as they intentionally were seeking it out. This contention is logically untenable and unpersuasive on its face.

---

[8](...continued)
and receipt of child pornography, the government's contention that the standards for the former (i.e., possession) are more stringent than for the latter (i.e., receipt) is open to serious question. Some courts have taken the view that knowing possession—even if fleeting—is an essential predicate for knowing receipt. *See United States v. Davenport*, 519 F.3d 940, 943 (9th Cir. 2008) ("It is impossible to 'receive' something without, at least at the very instant of 'receipt,' also 'possessing' it."); *United States v. Miller*, 527 F.3d 54, 71 (3d Cir. 2008) ("[I]t is clear that, as a general matter, possession of a contraband item is a lesser-included offense of receipt of the item."); *Romm*, 455 F.3d at 1001 ("Generally, federal statutes criminalizing the receipt of contraband require a 'knowing acceptance or taking of possession' of the prohibited item."); *United States v. Kamen*, 491 F. Supp. 2d 142, 150 (D. Mass. 2007) ("Receipt equals possession plus the additional element of acceptance, rendering possession a lesser included offense of receipt . . . ."); *cf. also United States v. Morgan*, 435 F.3d 660, 662–63 (6th Cir. 2006) (stating in dicta that a defendant who was initially charged with receiving child pornography under 18 U.S.C. § 2252A(a)(2) ultimately "entered an oral conditional plea of guilty to possessing images depicting minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252A(a)(5)(B), a lesser-included offense of the charged violation"). However, we need not definitively resolve that issue here. Even if we assume *arguendo* that significant distinctions exist between the proof requirements for child pornography possession and receipt offenses, we conclude that the government's arguments are unavailing.

The government also argues that in "a pure receipt case" it need not prove that the defendant "actually exercised control" over the illegal images, but rather "the ability to control the images he received is sufficient." *Id.* Even if it were true that in a receipt prosecution the focus is on the ability to control the images (rather than the actual control of them), that ability would need to relate to images that the defendant knew existed; otherwise, the defendant's conduct with respect to the images could not be deemed to be *knowing*. *Cf. Kuchinski*, 469 F.3d at 863 ("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." (emphasis added)). In other words, defendants cannot be convicted for having the ability to control something that they do not even know exists.

Generally, in regard to the cached images, the government failed to present any proof that Mr. Dobbs knew that the images were automatically being downloaded to his computer's cache—*viz.*, that he even knew that the images were there. Therefore, the government perforce failed to prove that Mr. Dobbs had the ability to control those images. As for any child pornography that may have appeared on Mr. Dobbs's computer monitor, the government's argument likewise breaks down when we specifically focus on the two images at issue.

The government presented no evidence that Mr. Dobbs actually saw the two images on his monitor, such that he would have had the ability to exercise control over them. As noted, the pattern of child-pornography-related searches immediately preceding the creation of illegal images in the cache does not apply to the two images submitted to the jury. In particular, the government's forensic specialist acknowledged that there was no evidence of suggestive searches immediately prior to the creation of those two images in the cache. Nor, according to the specialist, was there evidence of Mr. Dobbs visiting child pornography websites prior to the arrival of the two images in his cache. In sum, the lack of a search-and-creation pattern as it relates to the two images before the jury, when combined with the absence of any evidence establishing that Mr. Dobbs ever saw the images, forfends any view that *knowing* receipt could have been found by a rational jury. In other words, the government needed to present sufficient evidence in the first instance that Mr. Dobbs knew that the two images were present on his monitor before it could convict him of *knowingly* receiving them under its theory that receipt could be established in "a pure receipt case," Aplee. Br. at 29, by Mr. Dobbs's ability to control the images as they appeared on his monitor. It presented no such evidence here.

The government also highlights that Mr. Dobbs was charged with attempted receipt. Therefore, it reasons that we should not conclude that "the lack of direct evidence that Dobbs viewed the two images" is "fatal to his

conviction," because there was "substantial evidence establishing Dobbs's intent to receive child pornography, and that he acted to commit that offense" to permit us to "affirm his conviction on the attempt charge." Aplee. Br. at 32. In particular, as to the "substantial step" requirement of an attempt offense, the government contends that "the combination of those [Internet] searches [involving keywords suggesting child pornography] with Dobbs's subsequent visits to websites consistent with child pornography was precisely the type of act that would ordinarily result in the receipt of child pornography." *Id.* at 34.

However, when we pause to consider the nature of the completed offense that would necessarily need to be the object of any attempt conviction here, it is patent that the government's argument is unavailing. An attempt offense does not exist in a vacuum; it must relate to the completion of the charged offense. *See, e.g.*, *United States v. Cornelio-Pena*, 435 F.3d 1279, 1286 (10th Cir. 2006) ("A defendant is guilty of attempt if he intends to commit a crime and takes a substantial step toward the commission of *that* crime." (emphasis added)); *United States v. Taylor*, 413 F.3d 1146, 1155 (10th Cir. 2005) ("In our circuit, a conspiracy or an attempt to commit a crime requires the intent to commit the crime and overt acts in furtherance of *that intent*." (emphasis added)); *see also* Ira P. Robbins, *Double Inchoate Crimes*, 26 Harv. J. on Legis. 1, 70 (1989) ("Crimes in the nature of attempt, however, are not merely abstract attempts. Rather, they

are substantive offenses combining elements of a completed offense with *the attempt to commit that specific offense*." (emphasis added)).

Here, the only aspects of the charged offense that went to the jury involved two images—"b003[1].jpg," which was captured by the caching function on Mr. Dobbs's computer on March 15, 2006, at 9:29:56 p.m., and "14[2].jpg," which was captured shortly thereafter at 9:31:17 p.m. Thus, the government's evidence needed to be sufficient to establish the attempt offense *with respect to those two images*. Indeed, in oral argument, the government's counsel candidly acknowledged that, were the court to stray in its attempt analysis from a focus on the two images to the other images that the district court did *not* permit the jury to consider, it would "create problems." Oral Argument at 21:09.

In order to be guilty of attempt, a defendant must be shown to have intended to carry out the proscribed conduct—*viz.*, knowing receipt of child pornography. *See, e.g., Cornelio-Pena*, 435 F.3d at 1286 (stating that "to be guilty of attempt a defendant must intend to commit the crime"); *United States v. Evans*, 358 F.3d 1311, 1312 (11th Cir. 2004) ("A conviction for attempt require[s] proof . . . that [the defendant] possessed the *mens rea* required for the underlying crime . . . .").

Significantly, an essential element of an attempt offense is a "substantial step." *See, e.g., United States v. Munro*, 394 F.3d 865, 869 (10th Cir. 2005) ("To prove attempt, the government had to show that Munro took a 'substantial step'

towards the commission of the ultimate crime, and that such step was more than mere preparation."). Thus, the government's evidence had to be sufficient to prove that Mr. Dobbs took a substantial step toward the knowing receipt of the two images at issue. *See United States v. DeSantiago-Flores*, 107 F.3d 1472, 1479 (10th Cir. 1997) ("A substantial step is an 'appreciable fragment' of a crime and an action of 'such substantiality that, unless frustrated, the crime would have occurred.'" (quoting *United States v. Buffington*, 815 F.2d 1292, 1303 (9th Cir. 1987))), *overruled on other grounds by United States v. Holland*, 116 F.3d 1353, 1359 n.4 (10th Cir. 1997) (en banc footnote); *United States v. Savaiano*, 843 F.2d 1280, 1296 (10th Cir. 1988) ("We concluded that '[t]here must be an overt act pointed directly to the commission of the crime charged.'" (alteration in original) (quoting *United States v. Monholland*, 607 F.2d 1311, 1320 (10th Cir. 1979))).

In some instances, "[d]efining conduct which constitutes a 'substantial step' toward commission of the crime has proved to be a thorny task." *Savaiano*, 843 F.2d at 1296. However, on this record, it is not. As it pertains to the two images at issue, the government's evidence of a substantial step is clearly insufficient. As noted, the pattern of child-pornography-related searches immediately preceding the creation of the illegal images in the cache of Mr. Dobbs's computer does not apply to the two images submitted to the jury. Moreover, the government's forensic specialist acknowledged that there is no evidence of suggestive searches immediately prior to the creation of those two

images. And, there is no indication that Mr. Dobbs visited suspect websites before the images arrived in his computer's cache. Therefore, consistent with Mr. Dobbs's argument, we would be hard-pressed to conclude that Mr. Dobbs took a substantial step toward the knowing receipt of these two images, even if receipt could be accomplished through viewing the child pornography images on his monitor, with the present ability to control them. *See* Aplt. Reply Br. at 20–21 ("Yet [the government's] laundry list of facts returns to the evidence supporting the 15 images never submitted to the jury, namely, the searches he conducted to find them and the Web sites he visited to obtain them. None of these facts constitute a substantial step toward acquiring and controlling (that is, receiving) the two relevant images." (citation omitted)). Therefore, the government's attempt argument must fail.

III. Conclusion

For the reasons discussed above, we conclude that the government provided insufficient proof to establish the knowledge required for conviction under 18 U.S.C. § 2252(a)(2). Accordingly, we **REVERSE** the district court's judgment and remand with instructions to **VACATE** the conviction and sentence.

No. 09-5025, *United States v. Dobbs*

BRISCOE, Chief Judge, dissenting:

I respectfully dissent. In my view, the evidence presented by the government at trial was sufficient to allow the jury to find that Dobbs knowingly received or attempted to receive the two images at issue ("14[2].jpg" and "b003[1].jpg"), and that the two images were transported in interstate commerce. Thus, I would affirm Dobbs' conviction and resulting sentence.

I. Standard of Review

Although the majority correctly recites the basic standard of review that applies to Dobbs' sufficiency-of-evidence challenges, that standard bears repeating: "In reviewing sufficiency challenges, we ask whether, viewing the evidence in the light most favorable to the government as the prevailing party, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." United States v. Hutchinson, 573 F.3d 1011, 1033 (10th Cir. 2009) (emphasis added). It also is useful to note an accompanying standard that we have long employed, but that the majority has overlooked: "The evidence necessary to support a verdict 'need not conclusively exclude every other reasonable hypothesis and need not negate all possibilities except guilt.'" United States v. Wilson, 182 F.3d 737, 742 (10th Cir. 1999) (quoting United States v. Parrish, 925 F.2d 1293, 1297 (10th Cir. 1991) (citations omitted)). With

those standards in mind, I now turn to the arguments asserted by Dobbs in his appeal.

II. Sufficiency of evidence - knowing receipt

Dobbs first contends that the evidence presented at trial was insufficient to allow the jury to reasonably find that he "knowingly" received or attempted to receive the two images at issue. In addressing this contention, I begin first with the statute of conviction, then proceed to address the evidence presented by the government at trial, and conclude by addressing the two specific arguments raised by Dobbs on appeal. Finally, following the discussion of Dobbs' arguments, I shall outline what I see as the flaws in the majority opinion.

Dobbs' conviction arose under 18 U.S.C. § 2252(a)(2), which provides that any person who

> knowingly receives . . . any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, if—
>
> (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
>
> (B) such visual depiction is of such conduct;
>
> . . .
>
> shall be punished as provided in subsection (b) of this section.

18 U.S.C. 2252(a)(2) (2006).

The statute does not define the terms "knowingly" or "receives," "but in interpreting the[se] term[s], we are guided by [their] ordinary, everyday meaning." See United States v. Tucker, 305 F.3d 1193, 1204 (10th Cir. 2002). The district court instructed the jury that "[t]he term 'knowingly,' as used in the[] instructions, means that an act was done, or visual depictions were received, voluntarily and intentionally, and not because of mistake or accident." ROA, Vol. I at 340. In turn, the district court instructed the jury that "[t]he term 'receive' means to accept an object and to have the ability to control it." Id. These definitions, neither of which were challenged by the parties, comport with the terms' natural, ordinary meanings. E.g. United States v. Bowling, 619 F.3d 1175, 1184 (10th Cir. 2010) (affirming use of jury instructions that employed similar definition of "knowingly"); United States v. Stanley, 896 F.2d 450, 451 (10th Cir. 1990) (approving of district court's definition of "to receive" under § 2252(a)(2) as "to acquire control, in the sense of physical dominion or apparent legal power to dispose of the [object]"). Thus, I will employ these same definitions in analyzing whether Dobbs knowingly received or attempted to receive the two images at issue.

The government based its proof of Dobbs' knowing receipt on the testimony of Jonathon Bridbord, a computer forensic specialist employed by the United States Department of Justice's Child Exploitation and Obscenity section. Bridbord testified that his investigative task was to create and examine a "forensic

bit-stream image," or exact copy, of the contents of the hard drive of Dobbs' computer in order to determine if any "child exploitation offenses" existed on the hard drive. ROA, Vol. 3 at 127-28. Before discussing his specific findings, Bridbord described for the jury, in general terms, what would have occurred each time Dobbs accessed the internet with his computer. According to Bridbord, when a computer user such as Dobbs utilizes Microsoft Windows Internet Explorer (the browser) to access a particular web site, the browser in turn directs the computer to contact the web site's server (a dedicated computer holding the web site's content). The server then transmits, and the user's computer receives, the data and images associated with a particular page of the web site. In addition to displaying the images on the user's computer monitor, the browser also creates a copy of each image on the page and deposits it into what is referred to as the temporary internet files folder (or cache). In other words, absent the presence of unusual circumstances, such as the occurrence of a pop-up or the existence of malicious software, an image cannot be simultaneously displayed on the computer monitor and copied into the cache without the user accessing a web site on which the image is contained. A computer utilizing a Windows-based operating system (such as Dobbs' computer, which utilized the Windows XP Professional operating system) also creates an entry in what is referred to as the index.dat file, noting the date and time the web site was accessed. Lastly, if such a user employs a search engine, such as Google, to search for images or data, the user's computer records

each search term utilized, along with the date and time the term was utilized, into a file called the "Windows Registry." Id. at 209.

According to Bridbord, Dobbs first began using his Windows-based computer on November 15, 2005. Id. at 255. Bridbord testified that he determined, based upon his review of the files on Dobbs' computer, that Dobbs began performing Google searches for images of child pornography on December 15, 2005. Id. at 290. On that date, Bridbord testified, Dobbs used the search terms "ls-island," "ww2.ls-island.net," "www.ls-island.net," "ls-magazine," "ww2.ls-magazine/net," and "ww2.ls-magazine.net." Id. at 211. According to Bridbord, the term "ls" is an abbreviation commonly understood in the law enforcement community as an abbreviation for "Lolita Studios," and is associated with images of child pornography. Id. Bridbord testified that Dobbs continued to conduct searches for child pornography in late December 2005 (using the search phrase "very young sex"), February 2006 (using the search terms "young blowjob video," "ls-island.info," "lolita top," and "lolita new"), early to mid-March 2006 (approximately March 5 through March 12) (using the search terms "pedo," "erotic preteen," "erotic pre-teen," "pretty teen sex," "youngest porn," "young models," "pre teen sex," "priteen sex," "priteen newsgroups," "top preteen models," "lolita models," "pretene models," "pedo," and "pedo pics"), and early April 2006 (using the search terms "youngest cock sucker -gay," "pedo sex," "lolita blowjobs," "youngest cock sucker," "preteen models," "young cock

sucker," "young blowjob bbs," "preteen lolita," "preteen newsgroups," "lola," "nymphet," and "nymphet pics"). Id. at 291-93. In employing these search terms, Dobbs often advanced his browser numerous times in order to view additional search results (for example, Dobbs advanced his browser approximately thirty-six times when employing the term "preteen lolita"). ROA, Gov't Exh. 1.4 at 32.

Bridbord also provided information about specific web sites visited by Dobbs. One of the exhibits prepared by Bridbord and admitted at trial, Government Exhibit 1.6, listed the web sites visited by Dobbs between November 15, 2005, the date Dobbs first began using his computer, and the time the computer was seized by law enforcement officials in April 2006. Those entries, based upon the index.dat file of Dobbs' computer, indicated that Dobbs began visiting web sites that were potentially related to child pornography in late December 2005. ROA, Gov't Exh. 1.6 at 1-2. Similar web site visits occurred in February 2006, id. at 3-5 (indicating a number of such web sites visited on February 10, 2006), March 2006, id. at 6, 9-10, 16-19, and April 2006, id. at 21-26, 28-29, 33-42. Notably, those visits were not always associated with Dobbs' Google searches for child pornography images. In other words, the index.dat file entries indicated that, on some occasions, Dobbs directly visited potential child

pornography web sites without first employing a search engine or any child pornography-related search terms.[1]

Bridbord proceeded to describe for the jury seventeen images of child pornography he found in the cache of Dobbs' computer[2], including the two images that formed the basis of Dobbs' conviction.[3] The first image at issue, which had a file name of "b003[1].jpg," was created on March 15, 2006, at 9:29:56 p.m. The second image at issue, with a file name of "14[2].jpg," was created approximately a minute-and-a-half later, at 9:31:17 p.m. on March 15, 2006. For these two image files to have been created in the cache of Dobbs' computer, Bridbord testified, Dobbs "certainly ha[d] to visit a Web site or use another type of technology." ROA, Vol. 3 at 301. Bridbord testified, however, that he was unable to identify, based upon his review of the index.dat file, the

---

[1] According to Bridbord, it is not unusual for pedophiles to discover child pornography web sites through avenues other than search engines. ROA, Vol. 3 at 368.

[2] Bridbord testified that Dobbs' browser was set to retain only a certain amount of data in the cache, thus resulting in the automatic deletion of older files. ROA, Vol. 3 at 368. Consequently, Bridbord testified, it was possible that additional images of child pornography were received by Dobbs on his computer, but were not recoverable after the computer was seized by law enforcement authorities. Id. at 368-69. Indeed, Bridbord testified, he was able to identify the existence of "a number of files that were overwritten that were picture files," but was unable to completely recover those files. Id. at 369.

[3] The district court ruled, at the conclusion of the government's evidence, that the government failed to present sufficient evidence to allow the jury to find an interstate nexus for the other fifteen images. That ruling has not been challenged in this appeal.

web sites from which the two images were derived. Id. at 302-03. Bridbord explained that there are occasions when "data doesn't get written from the memory on to [sic] the hard drive," id. at 297, as well as times when the "data gets overwritten and the data is gone," id. at 272, thus forcing him "to piece together what's there," id. at 297. Bridbord ruled out the possibility that the two images at issue arrived in the cache of Dobbs' computer by way of "pop-ups" or malicious software. Id. at 254, 255, 257, 264, 371. Bridbord also noted that, immediately following the creation of the two images at issue, Dobbs directly visited four web sites associated with child pornography and that, as a consequence of that action, eight additional images of child pornography were copied into the cache of his computer. In sum, Bridbord opined, based upon a combination of his experience and his analysis of Dobbs' computer, that Dobbs' receipt of the two images at issue was the result of him "methodically seeking out child pornography." Id. at 222.

I readily conclude that Bridbord's testimony and related exhibits were sufficient to allow the jury to find that Dobbs knowingly received the two images.[4] As noted, Bridbord's analysis of Dobbs' computer established that, from

[4] Dobbs effectively concedes on appeal, as he did at trial, that he "received" the two images at issue. More specifically, Dobbs concedes: "1) that at various times he used his web browser to search for images of child pornography; (2) that he visited websites known to contain child pornography, and that some of these visits followed closely on the heels of his searches for child pornography; and 3) that images depicting child pornography were

(continued...)

late December 2005 through April 2006, Dobbs methodically utilized Google searches to locate images of child pornography (employing various search terms and often advancing his browser numerous times to produce additional search results), and directly visited numerous web sites whose addresses strongly suggested an association with child pornography. Bridbord's analysis further revealed that, as a result of this activity and the computer's automatic caching process, multiple images of child pornography were copied into the cache of Dobbs's computer, including the two images at issue. Considered together, I conclude that this evidence allowed the jury to find beyond a reasonable doubt that Dobbs knowingly sought and received the two images at issue by accessing web pages on which copies of those images were contained.[5] See United States v. Romm, 455 F.3d 990, 998 (9th Cir. 2006) ("In the electronic context, a person can receive and possess child pornography without downloading it, if he or she seeks it out and exercises dominion and control over it.").

Dobbs raises two specific concerns, neither of which give me pause. First, Dobbs correctly notes that the government offered no direct proof that either of

---

[4](...continued)
discovered on his computer." Aplt. Br. at 22.

[5] I acknowledge that if a defendant accidentally views a pornographic image, "as through the occurrence of a 'pop-up,'" that image will be copied into the computer's cache. United States v. Romm, 455 F.3d 990, 1000 (9th Cir. 2006). In light of the government's expert computer analysis in this case, however, I conclude the jury could have readily rejected the possibility that the two images at issue were accessed by Dobbs accidentally.

the two images actually appeared on his computer monitor. I am not persuaded, however, that such direct proof, which would be nearly impossible for the government to muster given the obviously secretive nature of the charged crime and the limitations of computer forensic science, was essential or, for that matter, required in order to support a conviction under 18 U.S.C. § 2252(a)(2). Given Dobbs's pattern, both before and after the receipt of the two images at issue, of methodically searching for images of child pornography and visiting web sites with an association to child pornography, I conclude the jury could have reasonably inferred that Dobbs was similarly methodical in actually viewing any web sites that he accessed that might have contained such images.[6] In other words, I conclude the jury could have reasonably inferred that Dobbs would have, in his search for child pornography images, methodically scrolled down the entire length of each web page he accessed, including the pages that contained the two images at issue.[7]

---

[6] The district court properly instructed the jury that it could base its findings upon either direct or circumstantial evidence, and could draw reasonable inferences from the evidence. ROA, Vol. I, Part 2 at 329.

[7] Even if I were to conclude the evidence presented at trial was insufficient to allow the jury to reasonably find that Dobbs actually viewed the two images on his computer monitor, I readily conclude that the evidence was more than sufficient to establish that Dobbs attempted to receive the two images at issue. More specifically, this evidence would have permitted the jury to reasonably find that (a) Dobbs intended to locate and receive images of child pornography, and (b) took a substantial step towards commission of that crime by intentionally accessing the web pages on which the two images at issue were contained. See

(continued...)

The second concern raised by Dobbs is that the government offered no evidence from which the jury could infer that he knew about his computer's cache or the caching process. Although this is true, I am not persuaded that such proof was required in order for the jury to convict Dobbs of knowing receipt of the images. As I see it, the government's evidence established that Dobbs's intent was to seek out and view images of child pornography. And this activity, which according to Bridbord afforded Dobbs temporary dominion and control over the images, was sufficient to establish his knowing receipt of the images. See Romm, 455 F.3d at 1000 (concluding that defendant "exercised control over the cached images while they were contemporaneously saved to his cache and displayed on his screen" because, "[a]t that moment," he "could print the images, enlarge them, copy them, or email them to others"). Thus, it was irrelevant whether Dobbs was aware of the computer's cache or the caching process, and the existence of copies of the images in the cache of his computer was, like fingerprints left at the scene of a crime, merely evidence of his actual criminal activity.

Having disposed of Dobbs' arguments, it is necessary to outline what I view as significant flaws in the majority's reasoning. Initially, the majority incorrectly suggests that the government's case rested exclusively on "a pattern . . . wherein the arrival of suspect images on Mr. Dobbs' computer was immediately

---

[7](...continued)
generally United States v. Ramirez, 348 F.3d 1175, 1180 (10th Cir. 2003).

preceded by searches using terms typically affiliated with child pornography." Maj. Op. at 5. Although Bridbord's testimony and related exhibits established that Dobbs sometimes utilized this pattern, that same evidence established that Dobbs frequently visited child pornography web sites directly, i.e., without any preceding searches. Indeed, the evidence established that, within two minutes of the creation of the second image at issue in this case, Dobbs directly visited four child pornography web sites and received eight additional images of child pornography. Moreover, Bridbord testified that it is not unusual for persons interested in child pornography to learn about child pornography web sites through avenues other than search engines. As for his inability to identify precisely what web site(s) Dobbs visited in obtaining the two images at issue, Bridbord explained that there are occasions when "data doesn't get written from the memory on to the hard drive," ROA, Vol. 3 at 297, as well as times when the "data gets overwritten and the data is gone," id. at 272. Finally, Bridbord ruled out the possibility that the two images arrived in Dobbs' cache as the result of pop-ups or malicious software. In sum, the lack of evidence of any Google searches immediately preceding Dobbs' receipt of the two images at issue is by no means fatal to the government's case, because Bridbord's testimony and related exhibits, taken as a whole, would have allowed the jury to reasonably conclude that Dobbs obtained the two images at issue by directly visiting child pornography web sites.

The majority also wrongly concludes that evidence of Dobbs' frequent "pattern of [employing] child-pornography-related searches immediately preceding the creation of illegal images in the cache" of his computer "is irrelevant to the question of whether [he] knowingly received the two images that were properly before the jury." Maj. Op. at 11. Dobbs' pattern of searching for and/or directly visiting child pornography web sites, which occurred both before and after the two images at issue were received on Dobbs' computer, as well as his receipt of other images of child pornography, was highly relevant for purposes of proving both absence of mistake and knowledge. See Fed. R. Evid. 404(b) ("Evidence of other crimes, wrongs, or acts . . . may . . . be admissible for . . . purposes [of proving] . . . knowledge . . . or absence of mistake or accident").[8] As I have already outlined, it was precisely this pattern of methodical activity that would have allowed the jury to reasonably infer that, upon visiting a web site potentially related to child pornography, Dobbs would have methodically perused

[8] Much, if not all, of the evidence of Dobbs' computer activity was inextricably intertwined with evidence of the charged offense, and thus would not have been subject to Rule 404(b) analysis. See generally United States v. Parker, 553 F.3d 1309, 1314 (10th Cir. 2009) (noting that "intrinsic evidence," which is not subject to Rule 404(b), "is directly connected to the factual circumstances of the crime and provides contextual or background information to the jury"). Nonetheless, it is useful in this context to note that, as set forth in Rule 404(b), even extrinsic evidence of criminal activity can be relevant for proving absence of mistake and knowledge.

the entirety of the site in his search for images of child pornography, and thus would have knowingly received the two images at issue.[9]

In this same vein, the majority errs in concluding that, because there was no evidence that Dobbs knew of his computer's automatic-caching function, "the presence of the child pornography files in the cache of Mr. Dobbs' computer does not alone demonstrate—circumstantially or otherwise—his knowing receipt of those files." Maj. Op. at 13. Bridbord testified in detail about seventeen images of child pornography he found in the cache of Dobbs' computer, including the two images at issue. With one exception, all of those images were copied into the cache at different times, thus indicating, according to Bridbord's testimony, that on each of those occasions Dobbs visited separate web sites containing images of child pornography. ROA, Gov't Exh. 1.12 at 1. Whether or not this evidence was sufficient, standing alone, to establish that Dobbs knowingly received the two images at issue, it was certainly relevant to that question. For example, this evidence would have supported a finding that the two images at issue arrived in the cache as a result of intentional activity on the part of Dobbs, rather than, as

[9] Although the majority takes the government to task for not presenting any evidence "establishing that Mr. Dobbs ever saw the images," Maj. Op. at 17, the majority fails to acknowledge the secretive nature of Dobbs' crime, and in turn fails to identify precisely what evidence it believes could or should have been presented. In any event, the majority also fails to explain why the jury could not reasonably have inferred, based upon the entirety of Bridbord's testimony and related exhibits, that Dobbs actually viewed the two images at issue.

suggested by his counsel at trial, by forces beyond his control and unbeknownst to him, such as pop-ups or malicious software.

Relatedly, the majority errs in suggesting that Dobbs' lack of knowledge of the automatic-caching process was fatal to his prosecution. The focus of Dobbs' internet activity was obviously to find and view images of child pornography, not to create copies of those images in his computer's cache. In turn, the knowing receipt issue hinged on whether Dobbs intentionally sought out and viewed the two images at issue. The fact that copies of the two images were found in his cache (along with other images of child pornography) was merely proof of that activity. In other words, Dobbs' awareness of the cache or the automatic-caching process was unnecessary to his conviction.

Similarly, the majority wrongly asserts that, because the government presented no proof Dobbs was aware of the cache or the automatic-caching process, it "perforce failed to prove that [he] had the ability to control those images." Maj. Op. at 16. As Bridbord explained, however, images displayed on a computer user's monitor can be manipulated, and thus controlled, by the user (for example by copying those images into a personal folder). ROA, Vol. 3 at 305, 354. Consequently, Dobbs' crime was complete at the moment he viewed the images on his monitor because, at that moment, he necessarily had the ability to control the images, regardless of whether or not he exercised control. See Romm, 455 F.3d at 1000 (reaching similar conclusion).

Finally, the majority errs in concluding that the government's evidence was insufficient to establish, for purposes of the attempt charge, that "Dobbs took a substantial step toward the knowing receipt of the two images at issue." Maj. Op. at 20. As with its analysis of the receipt charge, the majority wrongly refuses to acknowledge that it was entirely permissible for the jury to infer that Dobbs directly visited, with the intent of finding and viewing images of child pornography, web sites containing the two images at issue. More specifically, the jury could have based such a finding on the entirety of Dobbs' internet activity, Bridbord's explanation for why he could not identify the web sites from which the two images at issue were derived, and Bridbord's refutation of Dobbs' theory that the two images may have resulted from pop-ups or malicious software. Such a finding by the jury, which I submit could have been the only reasonable finding it could have made based upon the government's evidence, clearly would have satisfied the substantial step element of the attempt charge.

In sum, I conclude the evidence presented by the government at trial was sufficient to establish that Dobbs knowingly received, as well as attempted to receive, the two images at issue.

III. Sufficiency of evidence - travel in interstate commerce

Dobbs also contends that the evidence presented at trial was insufficient to establish the jurisdictional element for knowing receipt of child pornography under § 2252(a)(2), i.e., that the two images at issue traveled in interstate or

foreign commerce. Indeed, Dobbs argues that we are bound by our prior decision in United States v. Wilson, 182 F.3d 745 (10th Cir. 1999), to rule in his favor on this issue.

It is important to note that Wilson involved a different charge than the one at issue in the present case. In Wilson, the defendant was indicted for possessing three or more matters (one computer hard drive and ten computer diskettes) containing visual depictions of child pornography "which were produced using materials that had been mailed, shipped, or transmitted in interstate or foreign commerce in violation of 18 U.S.C. § 2252(a)(4)(B)." Id. at 740. At trial, a government witness testified that some of the images on the defendant's computer diskettes originated in German magazines. Id. at 744. We concluded that "the fact that some of the images possessed by defendant originated at some point in German magazines does not demonstrate, without more, that the German magazines were actually 'materials' used to produce the images possessed by defendant." Id. at 744 n.5.

But the instant case is distinguishable from Wilson because the government in this case, unlike in Wilson, did not seek to prove that the materials used to produce the images traveled in interstate commerce. Rather, the government in this case sought to prove that the visual depictions had traveled in interstate commerce, relying on the statutory language that prohibits knowing receipt of "any visual depiction that has been mailed, or has been shipped or transported in

interstate or foreign commerce . . . ."§ 2252(a)(2). This is a different jurisdictional prong than that relied on in Wilson.

Although Dobbs contends that the differences in statutory language are meaningless, I disagree. There is a significant difference between the materials used to produce visual depictions and the visual depictions themselves. They are independent jurisdictional prongs, either one of which the government must prove. See Wilson, 182 F.3d at 744 ("[T]he language of § 2252(a)(4)(B) makes it abundantly clear that either the visual depictions . . . or the materials used to produce the visual depictions must have traveled in interstate commerce."). Wilson focused on whether there was sufficient evidence to show that the materials used to produce the visual depictions had traveled in interstate commerce because the defendant in that case was charged under that jurisdictional prong. See id. at 740. Thus, Wilson does not answer the question presented under the jurisdictional prong in this case: whether proving the origin of photographs is sufficient evidence to prove that those visual depictions have traveled in interstate commerce.

The government in this case notes that it presented uncontroverted evidence that the two images at issue were originally created in Florida and New York, thus allowing the jury to reasonably find that, to end up on Dobbs's computer in Oklahoma, the images necessarily had to have traveled in interstate commerce. Dobbs argues, in response, that the government's theory is foreclosed by United

States v. Schaefer, 501 F.3d 1197 (10th Cir. 2007). In particular, Dobbs relies on the following language in Schaefer:

> [E]ven if we assume arguendo that the images appearing in the foreign language movie clips and the image of the young girl originated outside of the State of Kansas (like the images from the German magazine in Wilson), the government offered no proof that the particular images on the CDs in question moved across state lines.

Id. at 1206.

I conclude that Dobbs's reliance on Schaefer is misplaced. There was no evidence in Schaefer supporting where the images at issue there originated. Rather, the government's only evidence was that the defendant had (a) used the internet, and (b) possessed CDs that contained images of child pornography. Id. at 1198. We declined to assume "that Internet use automatically equates with a movement across state lines." Id. at 1205. Specifically, we held "that the government's evidence concerning [the defendant's] use of the Internet, standing alone, was insufficient to satisfy the jurisdictional requirements of these statutes." Id. at 1207. Notably, we were not presented with a case where the government provided any other evidence of a jurisdictional nexus, such as evidence of the origin of an image. Moreover, we have since recognized that "Schaefer is limited to its facts–the government's say so was not enough to prove that the Internet operates in interstate commerce, no matter how obvious." United States v. Vigil, 523 F.3d 1258, 1266 (10th Cir. 2008).

I thus address head-on whether evidence of the out-of-state origin of a photograph, as was presented by the government in this case regarding the two images at issue, is sufficient evidence to meet the jurisdictional requirement of § 2252(a)(2). Dobbs argues that evidence of the origin is insufficient for two reasons. First, the government did not prove an interstate internet connection. And second, even if the government proved where the original photograph was taken, this does not prove that the "particular" images found in Dobbs's cache traveled in interstate commerce. See Aplt. Br. at 47.

I turn first to Dobbs's argument that Schaefer requires the government to prove an interstate internet connection. As I have explained, Dobbs's reliance on Schaefer is misplaced. In that case, we recognized that the government needed to prove that the images in question had moved between states, and proof of an internet connection, by itself was insufficient. See Schaefer, 501 F.3d at 1206. We noted that "the government offered no proof that [the defendant] accessed the images through an interstate Internet connection." Id. That is not the same as requiring an interstate internet connection in every case in order to prove that an image has crossed state lines. While proof of an interstate internet connection may be sufficient to show that an image crossed state lines, it is not always necessary. Rather, the government must prove that the visual depictions traveled in interstate commerce at some point prior to arriving on Dobbs's computer. See United States v. Snow, 82 F.3d 935, 941 (10th Cir. 1996) (concluding that

jurisdictional requirement that a firearm was "shipped or transported in interstate commerce" was met upon proof that "firearm had at some point crossed a state line."); see also United States v. Urbano, 563 F.3d 1150, 1154 (10th Cir. 2009) (recognizing sufficient jurisdictional nexus when firearm traveled in interstate commerce at some time in the past). An interstate internet connection is but one way to prove that the image traveled in interstate commerce.

I next address Dobbs's argument that the government can prove only where the original photographs were taken, not where the "particular" images found on his computer came from. To answer this question, I must decide whether the statute distinguishes between original images and copies of those images when regulating visual depictions that have traveled in interstate commerce.

I begin with the statutory language, giving the words their ordinary or natural meaning. Wilson, 182 F.3d at 740. The effective statute refers to visual depictions that have been transported in interstate or foreign commerce "by any means including by computer." § 2252(a)(2). As the government explains, when one computer sends a digital image to another computer, "the original image does not travel from the sender to the recipient. Rather, the original remains on the sender's computer, and an exact digital copy is created on the recipient's computer." Aplee. Br. at 43. Thus, any transmission by computer necessarily involves the creation of copies.

Dobbs's suggestion that the statute covers only "particular" images but not copies would render the statutory language "by any means including by computer" meaningless. But, federal courts "cannot construe a statute in a way that renders words or phrases meaningless, redundant, or superfluous." United States v. Power Eng'g Co., 303 F.3d 1232, 1238 (10th Cir. 2002). Because the statutory language explicitly includes "by computer," and computers necessarily create digital copies when they transmit images, it follows that the statute covers copies of a visual depiction, and not merely the original visual depiction itself.

I am thus left to decide whether the evidence presented at trial was sufficient to prove that the two images submitted to the jury traveled in interstate commerce, "by any means including by computer." Taking the evidence in the light most favorable to the government, I have little trouble concluding that a reasonable jury could find that an image originally created in New York or Florida necessarily had to have traveled in interstate or foreign commerce before arriving on a computer in Oklahoma. See United States v. Schene, 543 F.3d 627, 639 (10th Cir. 2008) (holding that there was sufficient evidence to prove that a hard drive was a "material" that had traveled in interstate or foreign commerce upon proof that the hard drive was manufactured in Singapore); see also United States v. Williams, 403 F.3d 1188, 1195 (10th Cir. 2005) (holding that there was sufficient evidence that a firearm had previously traveled in interstate commerce by proof that the firearm was manufactured out-of-state).

I note that this conclusion is supported by our prior unpublished decision in United States v. Swenson, No. 07-8097, 2009 WL 1803285 (10th Cir. June 25, 2009). In Swenson, the defendant was convicted for receipt, possession, and attempted distribution of child pornography under §§ 2252A(a)(2) and 2252A(a)(5)(B). Id. at *1. There, state agents in Wyoming discovered that the defendant was offering images of child pornography for download via Limewire, a peer-to-peer networking application. Id. At trial, the government introduced evidence that at least one image was being distributed out of South America. Id. at *2. We concluded that "[a] reasonable jury could (even if it need not) conclude from this evidence that, for the image to wend its way from South America to Wyoming, it had traveled in interstate or foreign commerce . . . ." Id. While certainly not binding, the Swenson decision is persuasive regarding what a reasonable jury could conclude when given virtually the exact same evidence as that presented to the jury in the case at bar.

In sum, I conclude that because a reasonable jury could find that the two images at issue traveled in interstate commerce at some point before arriving on Dobbs's computer, there was sufficient evidence to support the jurisdictional element.

I would affirm Dobbs' conviction and sentence.