IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

United States Court of Appeals
Fifth Circuit
FILED
April 25, 2011

Lyle W. Cayce
Clerk

No. 09-50703

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

DAVID WINKLER,

Defendant - Appellant.

Appeal from the United States District Court
for the Western District of Texas

Before GARWOOD, ELROD, and SOUTHWICK, Circuit Judges.

JENNIFER WALKER ELROD, Circuit Judge:

David Winkler appeals from two counts of his four-count conviction for receipt and possession of child pornography, challenging the sufficiency of the evidence supporting his conviction. Primarily, he argues that his conviction for knowing receipt of child pornography cannot stand because it was based on

images found only in the temporary storage of his computer hard drive. We now AFFIRM.

I.

Winkler's name came to the attention of law enforcement during two national investigations led by elements of Immigration and Customs Enforcement (ICE) during 2005 and 2006. The first, "Operation Emissary," was initiated in 2005. That investigation led to the discovery of a child pornography website. In order to access that website, a potential user visited a welcome page that offered samples of child pornography, and unlimited memberships for $79.95 and $90.00 for twenty days and a month respectively. Once a purchase had been made, the user would receive an email from an unrelated address a day later containing a link to the illicit content. Following the link led to a sign-in screen which required a username and password, after which the website warned that its contents were illegal in all countries. Evidence at trial established that after entering the website through those initial screens, a user could access approximately 1,000 images of child pornography, including videos. Having executed a search warrant for the physical internet server hosting the website, ICE agents discovered that the e-mail account of "dcwink@ktc.com" together with a zip code, city and street address, was transmitted to the website as part of a membership sign-up procedure. Agents then investigated payments made to the website. They found that a credit card belonging to David Winkler was used to make purchases of child pornography on two dates.

"Operation Flicker," a second ICE investigation initiated in 2006, focused on a specific commercial child pornography service which contained within it links to hundreds of individual child pornography websites. The agent in charge

of the investigation accessed the website to confirm that it contained child pornography, and also conducted undercover purchases of access to discover the contents of the various linked sites. In the course of his investigation, the agent determined that someone using a paypal account associated with David Winkler had purchased access to one of those linked sites.

David Winkler's name was then referred to local ICE agents in February 2007. By obtaining credit card records, those agents were able to determine that Winkler's credit card was used for transactions in the same dates and amounts that were discovered in the Operation Emissary and Operation Flicker leads. The credit card records verified those purchases and showed that they were never credited back to the account or disputed. ICE then executed search warrants for Winkler's home and office addresses. As a result of its investigation, ICE seized several computers and hard drives belonging to Winkler. Three of the seized hard drives are relevant to this case: the Quantum Fireball hard drive, the Seagate hard drive and the Maxtor hard drive.

Agent James Beard, a computer forensics agent, conducted a forensic investigation on each of those hard drives. He discovered images and videos of child pornography on all three. Specifically, Beard found 261 images of child pornography on the Quantum hard drive, 26 video files containing child pornography on the Maxtor hard drive, and 261 images and 18 videos containing child pornography on the Seagate hard drive. Many of the files found on the Quantum hard drive were located in the utilities CD-ROM toolkit extras folder, a folder normally dedicated to files related to the Apple CD-ROM toolkit application. As Beard testified, that was not a normal place for the computer to store files downloaded by the user, but rather a special directory reserved for

files associated with a specific hardware utility. To save a file there, an individual would have to browse his hard drive's contents and specifically choose that obscure directory. On the Seagate hard drive, most of the child pornography files were contained in the program files directory, in a folder entitled "wait2." That is also not a default location for user downloaded files. Moreover, Beard discovered a text file in the program files directory entitled "med study list." Instead of containing a list of medical publications as the file name indicates, however, the file contained links to child pornography sites.

As for the Maxtor hard drive, which contains all the child pornography specifically at issue in this appeal, Beard testified that he found two user accounts. The first was an account named "user" — which Winkler admits was intended for his use — and the second a "staff" account, used by Winkler's office staff. Both accounts were password protected, and the password for the "user" account was the same password Winkler used for his home computer. Beard testified that the "staff" account on the Maxtor hard drive did not contain any child pornography. In his forensic investigation of the "user" account, however, Beard found a total of 26 video files of child pornography.

Five of those video files were located in a temporary internet cache – where internet browser software automatically saved the content of visited websites for the purpose of reducing page-loading time if the user revisits the site – including the only two files alleged in Count One. Evidence elicited by the government showed that those two files had been downloaded from the "members only" section of a child pornography website. Beard further testified that a video file is copied to a temporary internet cache when the user takes an affirmative action such as clicking on the video in order to play it. Thus, Beard

explained, a video file differs as a technological matter from a still photo displayed on a web site, which is downloaded automatically to an internet cache when the web page it is displayed on is loaded.

The other 21 illicit videos were stored in various subfolders within the "mydocuments" folder of the Maxtor hard drive. Two of the files listed in Count Five were saved to the "lpack19vi" folder. Beard also discovered a zip file of the same name saved on the Maxtor hard drive. By cracking the password protecting the zip file, he discovered that those two files listed in Count Five had been extracted into the lpack19vi folder from that zip file. The other two video files listed in Count Five were saved to the "lpack20vi" and "lpack21vi" folders respectively. Beard testified that those video files also appeared to have been extracted from zip files of the same name as the directory in which they were saved. Beard testified that all four zip files he discovered on the Maxtor hard drive were downloaded to the Maxtor hard drive in the password protected "user" accounts between 9:49 pm and 9:56 pm on December 21, 2004.

In the course of his forensic investigation, Beard also checked whether any type of viruses or malware had infected the Maxtor hard drive. He found none. He also found no indication of remote access to the Maxtor hard drive that could indicate that a trojan or other kind of virus or invasive software downloaded illicit files to the hard drive without Winkler's knowledge.

As a result of the ICE investigation, Winkler was charged with receiving and possessing child pornography under 18 U.S.C. 2252(a)(2) and 18 U.S.C. 2252A(a)(5)(B), and his case was tried to a jury in 2009. He was convicted, and sentenced to 72 months imprisonment on Count One, and 73 months imprisonment on Counts Three, Four and Five, all to run concurrently, followed

by concurrent 15 year terms of supervised release on each count. No fine was imposed, but Winkler was ordered to pay a $100 special assessment as to each of the four counts of conviction. In this appeal, Winkler disputes only his convictions on Counts One and Five. Specifically, Count One alleges, under 18 U.S.C. 2252(a)(2), that Winkler "did knowingly receive" two video files depicting minor females engaging in sexual activity with adult males. Count Five alleges, under 18 U.S.C. 2252A(a)(B)(5), that Winkler "did knowingly possess" four video files depicting minor or prepubescent females engaging in sexual activity.

II.

Winkler makes two claims on appeal. First, he claims that because the images alleged in Count One were found only in his temporary internet cache, there was insufficient evidence to support his conviction for "knowingly receiving" those images under 18 U.S.C. 2252(a)(2). Second, he claims that the evidence at trial was insufficient to support his conviction, on Count Five, for possessing certain other images under 18 U.S.C. 2252A(a)(5)(B). In support of that argument, he offers various alternative explanations for the presence of the files on his hard drive, and also contends that the government failed to show that the images alleged in Count Five of his indictment traveled in interstate commerce.

A challenge to the sufficiency of evidence following a proper motion for acquittal is reviewed by this court de novo. *United States v. Valle*, 538 F.3d 341, 344 (5th Cir. 2008). In reviewing challenges to the sufficiency of the evidence in a criminal case, the evidence is viewed in the light most favorable to the jury verdict. *United States v. Resio-Trejo*, 45 F.3d 907, 910 (5th Cir. 1996). All credibility determinations and reasonable inferences from the evidence are to be

resolved in favor of the jury verdict. *Id.* at 911. Moreover, a court "must affirm if a rational trier of fact could have found that the evidence established the essential elements of the offense beyond a reasonable doubt." *United States v. Lopez*, 74 F.3d 575, 577 (5th Cir. 1996). We address Winkler's arguments under that standard.

A. Winkler's Conviction for Knowing Receipt of Child Pornography

Winkler argues that his conviction for Count One must be set aside because the government failed to prove that he knowingly received the two files at issue.[1] He argues that the most the evidence shows is that he viewed those two videos over the internet, and that he was unaware that the files would be automatically downloaded into the temporary cache on his staff computer. Thus, he asserts that those facts cannot support a conviction for knowing receipt of electronic child pornography.

We disagree. To be sure, the exact contours of the crime of "knowingly receiving" electronic child pornography in a constantly shifting technological background are murky. Part of the problem is that computers connected to the internet store vast quantities of data about which many users know nothing. As a user browses the internet, the computer stores images and text and other kinds of data in its temporary memory the way a ship passing through the ocean collects barnacles that cling to its hull. Thus, there is some risk that the

[1] At the threshold the government argues that Winkler waived his claims on Count One of the indictment by omitting the argument he now makes from his oral motion for acquittal during trial. Thus, the government argues, his conviction must be reviewed under the stringent "manifest miscarriage of justice" standard. *See United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007). We need not decide that question, however, because we conclude that the evidence supports Winkler's conviction under the standard for the review of a jury's verdict.

computer of an internet user not intending to access child pornography may be infected with child pornography. Understandably, our sister circuits have struggled with whether to impute knowledge from the presence of illicit files found in such temporary storage.[2]

The Tenth Circuit recently reversed a conviction for knowing receipt of child pornography based entirely on two electronic photographs found only in the defendant's internet cache. *United States v. Dobbs*, 629 F.3d 1199, 1201 (10th Cir. 2011). The Tenth Circuit based its ruling on the fact that there was no evidence that the defendant had accessed the files stored in the computer's cache, and there was no evidence that the defendant knew of the computer's automatic-caching function or that the images had come to the defendant's computer as a result of a specific pornography related internet search – all the government could rely on was a general pattern of child pornography related searches. *See id.* at 1202 (noting that "there was no evidence of a temporally proximate search indicating the pursuit of child pornography with respect to the two images submitted to the jury"). There was no evidence that the defendant in *Dobbs* was a member of any pay-per-view child pornography website, or, indeed, that the

[2] The other problem that courts have grappled with, and which Winkler raises in passing, is the difference between the quantum of proof necessary to show "knowing receipt" of child pornography as opposed to what some courts have characterized as the lesser included offense of "knowing possession." *See, e.g., United States v. Miller*, 527 F.3d 54, 64 (3d Cir. 2008) (observing that "the quantum of evidence required to prove knowing receipt of a downloaded file may, in some situations, be greater than that minimally required to prove knowing possession of the file"). It is true, for example, that one may accidentally receive a file, and then, after consideration, decide to keep it, and thus be liable for knowing possession but not receipt. There may be other circumstances in which possession can be proven but receipt cannot. But that distinction is not at issue here, and we therefore need not opine on it now. *See United States v. Dobbs*, 629 F.3d 1199, 1206 (10th Cir. 2011) (declining to opine on the difference between knowing possession and knowing receipt).

defendant had *even seen* the two images that were the basis of his conviction. *Id.* at 1207. As the *Dobbs* court concluded: "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 [the defendant] ever saw the images, forfends any view that *knowing* receipt could have been found by a rational jury." *Dobbs*, 629 F.3d at 1207 (emphasis in original).

By contrast, in two other cases involving child pornography found in a user's internet cache, the Tenth Circuit upheld convictions where a review of the evidence showed that the evidence did point convincingly towards the defendant's intent. *See United States v. Bass*, 411 F.3d 1198 (10th Cir. 2005); *United States v. Tucker*, 305 F.3d 1193, 1204 (10th Cir. 2002). In *Bass*, the court relied on the fact that the defendant used software "specifically aimed at eliminating the digital residue of his illicit activities," *Dobbs*, 629 F.3d at 1205, to determine that the defendant did knowingly receive the files stored in his internet cache. *See Bass*, 411 F.3d at 1202. Similarly, the Tenth Circuit affirmed a conviction for possession where the defendant argued that he never intentionally saved the files in his cache to his hard drive. *See Tucker*, 305 F.3d at 1204. There, the court focused on the defendant's admission that he knew the images on the web page would be sent to his browser cache file. *Id.* Thus, the court held, because the defendant "knew his browser cached the image files, each time he intentionally sought out and viewed the child pornography with his web browser he knowingly acquired and possessed the images." *Id.* at 1205.

Other circuits have agreed that while "the specter of spam, viruses, and hackers must not prevent the conviction of the truly guilty . . . prosecutors, judges and juries have a duty to safeguard – as best as they are able – potential

defendants when receipt of child pornography might well have been truly inadvertent." *United States v. Pruitt*, No. 10-10829, 2011 WL 1380687, at *3 (11th Cir. Apr. 13, 2011) (not yet published). In *Pruitt*, the Eleventh Circuit affirmed a knowing receipt conviction for files held in a cache where the evidence showed that the defendant sought out and viewed child pornography, searched for child pornography on the internet, and had downloaded child pornography on an entirely different computer at the same time. *See Pruitt*, 2011 WL 1380687, at *3. In another child pornography possession case, the Ninth Circuit was faced with the question of whether thousands of images of child pornography stored in a temporary folder could be counted for the calculation of a defendant's sentencing guidelines range, thereby dramatically enhancing the defendant's sentence for 110 images held in permanent storage. *See United States v. Kuchinski*, 469 F.3d 853, 861-62 (9th Cir. 2006). Citing the fact that there was no evidence the defendant was a sophisticated computer user, that he tried to get access to the cache files, or that he knew of the cache's existence, the court answered in the negative: "[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." *Id.* at 863. As the court stated, to charge someone with possession and control over cache files without "some other indication of dominion and control over the images . . . turns abysmal ignorance into knowledge and a less than valetudinarian grasp into dominion and control." *Id.* at 863.

However, the Ninth Circuit has affirmed convictions where the evidence of knowledge was stronger than in *Kuchinski*. *See United States v. Romm*, 455 F.3d 990 (9th Cir. 2006). There, the court affirmed a conviction for files found in an

internet cache where the defendant admitted he destroyed images held in his cache. *Id.* at 990. In so holding, the court observed that the defendant "exercised control over the cached images while they were contemporaneously saved to his cache and displayed on his screen," contrasting that quantum of knowledge with the acquisition of images that occurs when "a defendant accidentally views the images, as through the occurrence of a 'pop-up.'" *Id.* at 1000.[3]

What unites these cases is not the cache as such, but rather the broader concern that an internet user may find himself ensnared in a child pornography case unwittingly, by virtue of files that were copied to temporary storage and never knowingly received. *Cf. United States v. Stulock*, 308 F.3d 922, 925 (8th Cir. 2002) (summarizing a district court's unchallenged observation that "one cannot be guilty of possession for simply having viewed an image on a web site, thereby causing the image to be automatically stored in the browser's cache"). The various proxies other courts have used to determine whether a defendant knowingly received the illicit material, whether it is the defendant's knowledge of the cache function, a search pattern for child pornography, evidence of deleting illicit files after the fact, or the use of cache cleaning software, all go to that central issue. But none of those factors is talismanic. The duty of the appellate

[3] This court's only directly relevant case, an unpublished disposition, is consistent with the decisions of our sister circuits. *See United States v. Calderon*, 318 Fed. Appx. 277 (5th Cir. 2009). There, we were faced with the question of whether files held only in an internet cache could be counted for the purpose of sentencing. *Id.* at 278. The defendant argued, on the basis of the Ninth Circuit's conclusion in *Kuchinski*, that such images could not be used. *Id.* We rejected that argument, noting that "there is ample evidence in this record to support the district court's determination that [the defendant] possessed the requisite images," including "a long-term history with child pornography. [the defendant's] activity procuring child pornography . . . and [the defendant's] lack of alternate explanations for the presence of images found on his computer." *Id.*

court is to discern, based on all the evidence, whether the jury could have found knowing receipt. As the cases in our sister circuits show, that inquiry is highly fact specific and not tied to whether the files at issue were found in a cache directory or, alternatively, in the user controlled portion of the hard drive. This reading of the statute not only comports with the ordinary, everyday meaning of the word "receive" – which we are bound to respect in the absence of an alternative statutory definition, *see United States v. Dickson*, 632 F.3d 186, 189 (5th Cir. 2011) – but also prevents savvy users of child pornography from using the technologically static nature of our opinions as a basis for engaging in precisely the behavior the anti-child pornography statutes were meant to forbid.

The facts in this case are far more like those in *Tucker*, *Bass*, *Romm* and *Pruitt* than those in *Dobbs* and *Kuchinski*. "The mere presence of the files in the cache is certainly proof that the files were *received*." *Dobbs*, 629 F.3d at 1205 (emphasis in original). The only question is whether that receipt was knowing. In stark contrast to *Dobbs* – where the evidence supporting the government's case was tenuous at best – the evidence from which a rational jury could infer that Winkler himself sought out, downloaded, viewed and had the ability to manipulate the images at issue in this case is overwhelming. Crucially, the government elicited evidence from which the jury could infer that the files at issue came from the members-only section of a child pornography site – the same source from which the files at issue in Count Five came. Given the evidence at trial, and especially the evidence that Winkler repeatedly paid for members-only child pornography sites, the jury could have concluded that Winkler paid for access to the child pornography website, entered a password and username to access the two videos in Count One, and had them transmitted to his computer.

Moreover, the jury heard that the only way those files could have been copied to the cache was by Winkler's decision to click and watch the videos, in contrast to the way the still photos at issue in *Dobbs* (and many of the other cases on which the parties rely) can arrive in the cache (for example, by accessing a web page on which there is child pornography without intending to access child pornography). Those facts completely differentiate this case from *Dobbs*.

The jury also heard testimony that Winkler had downloaded dozens of images of child pornography, and that the files he received from those sites were often hidden (albeit amateurishly) behind password walls in his own user account or in unnatural locations in the computer's file hierarchy rather than the normal location for downloaded material. The jury also heard that Winkler kept a catalogue of child pornography links, masquerading as a list of medical studies, in one of his hard drives. Those facts speak to a pattern of child pornography receipt and possession that could also have caused a rational jury to conclude that Winkler knowingly received the files in Count One. In sum, this is not the exceptional case in which the government has persisted in bringing a criminal prosecution against the unknowing victim of a computer's inner workings.

B. Sufficiency of the Evidence Supporting Count Five

Winkler makes a series of arguments disputing the proof the government adduced showing that he downloaded the files at issue in Count Five. He relies on a Wal-mart store receipt showing that he purchased several items with his credit card at 10:52 p.m. on December 21, 2004. He argues that because the government's evidence showed the illicit files in question were downloaded at 10:53 p.m. on the same day, "it would be impossible for him to be the person at the staff computer downloading the zip files at that time." Winkler also points

to other evidence in support of his innocence. For example, that there had been virus problems on that computer "several years ago," that he had not changed his password in twelve to fifteen years and that several cleaning crews and other individuals had access to his computer area over the years. He also argues that the government failed to show that there had been an after hours opening of his medical office on December 21, 2004 and thus the government presented no evidence that Winkler had entered his office late at night to access child pornography. Finally, Winkler argues that because he himself chose to present the staff computer for review by pre-trial forensic experts, it is not plausible that he was aware of child pornography on that computer.

Viewing the evidence in the light most favorable to the verdict, the Government produced sufficient evidence for a reasonable juror to find that Winkler knowingly downloaded the files at issue in Count Five. *See United States v. Percel*, 553 F.3d 903, 910 (5th Cir. 2008). As to the Wal-mart receipt, the government's forensic expert, James Beard, testified that the government exhibit Winkler disputes was improperly time-stamped. Viewed properly, he testified, the download occurred at 9:53 p.m., leaving plenty of time for Winkler to complete the download and proceed to Wal-mart to purchase items at 10:53 p.m. The jury was entitled to believe Beard on this point and not Winkler. As for his other claims, Winkler presented no evidence in support of his theory that his staff computer had been improperly accessed by a virus or through some other method, or that a member of his own staff or another doctor's had broken into his computer and downloaded child pornography. Similarly, Winkler's security records argument fails because, in the absence of any opening and closing security records for December 21, 2004, there was no basis for the jury to exclude

Winkler's presence. Rather, the jury was free to conclude, based on all the circumstances, that Winkler entered the office sometime on December 21 and downloaded the files in question. The jury could also have agreed with the government's argument that Winkler brought the staff computer to pre-trial services because he simply forgot it contained child pornography.

At most, Winkler posited plausible alternative explanations for how the illicit pornography came to be on his computer. But a jury is not required to accept *any* alternative explanation. *United States v. Moreno*, 185 F.3d 465, 471 (5th Cir. 1999) (noting that a jury is "free to chose among reasonable constructions of the evidence"). Rather, taking into account the overwhelming evidence the government presented of Winkler's involvement with child pornography, and that he purchased access to child pornography websites and downloaded child pornography, the evidence presented by the government was sufficient for the jury to reject the evidence presented by the defense, and to credit the prosecution's case.

Winkler also argues that his conviction on Count Five should be reversed because "the Government offered no evidence to show that any of the files alleged in Count Five had ever traveled on the Internet, or had otherwise moved in interstate commerce," and thus the government failed to prove the jurisdictional element of the crime. Winkler is incorrect. Evidence at trial established that the zip files housing the individual videos at issue in this count were obtained from a website. Evidence at trial further demonstrated the files at issue in Count Five were extracted from those zip files onto Winkler's hard drive, and thus that the files came to Winkler's computer from the internet. *See United States v. Runyan*, 290 F.3d 223, 242-43 (5th Cir. 2002) (affirming a conviction where the

government adduced adequate circumstantial evidence to tie particular images of child pornography to the internet). Therefore, the evidence at trial was sufficient to support Winkler's conviction on Count Five.

III.

For the foregoing reasons, Winkler's conviction is AFFIRMED.