

**IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT**

No. 12-50855

United States Court of Appeals
Fifth Circuit

FILED

November 13, 2013

UNITED STATES OF AMERICA,

Plaintiff - Appellee

Lyle W. Cayce
Clerk

v.

ETHAN NATHANIEL LARMAN,

Defendant - Appellant

Appeal from the United States District Court
for the Western District of Texas
USDC No. 3:11-CR-1007-1

Before JOLLY, JONES, and BARKSDALE, Circuit Judges.

PER CURIAM:*

Ethan Larman appeals his conviction on one count of Receipt of Child Pornography, one count of Attempted Distribution of Child Pornography, both under 18 U.S.C. § 2252A(a)(2), and two counts of Possession of Child Pornography under 18 U.S.C. § 2252A(a)(4)(B). Larman not only challenges the sufficiency of the evidence to convict him, but further asserts errors in jury instructions, an error in an evidentiary ruling, and errors in the application of

* Pursuant to 5TH CIR. R. 47.5, the court has determined that this opinion should not be published and is not precedent except under the limited circumstances set forth in 5TH CIR. R. 47.5.4.

No. 12-50855

two sentencing enhancements. We consider and reject his arguments, and, for the reasons that follow, we AFFIRM his conviction and sentence on all counts.

I.

On October 23, 2010, an Internet Protocol address (“IP address”) in El Paso, Texas, made available for sharing child sexual abuse images over a peer-to-peer network (“P2P”) between 8:12 and 8:57 a.m.¹ Law enforcement monitoring software created an activity report identifying the internet service provider (“ISP”) and the amount of images, categorized as “child notable,” associated with child abuse. Nicholas Marquez, a special agent with the Homeland Security Investigations Cyber Crimes Group (“HSI”), first observed this report on November 23, 2010, exactly one month after the incident of sharing. The software identified these images as “child notable” because of unique indicators called hash values, contained within the images’ source code. Hash values, specific to the makeup of a particular image’s data, allow law enforcement to compare suspected child sexual abuse images to ones already present in law enforcement media libraries. This comparison allows law enforcement to identify child pornography with almost absolute certainty, regardless of the name associated with a file.

Using this process, Marquez confirmed that thirteen images from the October 23 incident were indeed verified child sexual abuse images. After this confirmation, Marquez sent a summons to the ISP, Time-Warner Cable, requesting the subscriber information for that particular IP address. He received notice that the IP address belonged to Ethan Larman, a member of the U.S. military, at his El Paso, Texas address. Once Marquez confirmed that Larman resided at that address, he obtained a search warrant for Larman’s

¹ P2P programs allow computers to exchange information by connecting with one another without having to go through an IP server. On a P2P network, any data placed in a shared folder on a user’s computer can be accessed by anyone else using P2P software.

No. 12-50855

residence. Two days later, Marquez and other agents executed the warrant. While executing the warrant, agents took Larman and his roommate Benjamin Morgan outside while officers conducted a search of the apartment.

Once outside, Marquez and Dustin Sletner, a special agent in the U.S. Army Criminal Investigation Division, interviewed Larman inside a government vehicle. Sletner took detailed notes during this interview, although the purpose of his presence was to serve as a witness. Marquez and Sletner testified that Larman told them he owned a computer and that he was the only individual who used the computer. Larman described his expertise with computers as “low,” but he acknowledged that he knew how to move, delete, and rename files. Most importantly, Larman admitted downloading child pornography through the Limewire P2P program approximately 50 times beginning in June of 2010. Larman informed the two agents that there were incriminating images in the “My Pictures” folder on his computer, on his PlayStation 3, and on two thumb drives he owned. In addition to these admissions, Larman informed agents as to why he was attracted to underage girls and described the manner in which he ordinarily viewed the images. Larman would later testify at trial and deny telling the agents that he ever downloaded or possessed any child pornography.

The search of Larman’s apartment yielded five pieces of electronic media belonging to Larman that authorities suspected contained child pornography. HSI Special Agent Joseph Byers, a forensic examiner, examined the media using complex forensic software that creates a mirror image of the contents of a media device. The first device was an E-Machines desktop computer (named “C1H1”), found on the upper shelf of a closet in Larman’s bedroom. The second and third devices were two SanDisk thumb drives labeled “TD-1” and “TD-2,” respectively. The fourth device was a PlayStation 3, which Byers was unable to examine because of the device’s encryption technology. The final device was

No. 12-50855

a CD-R with the word “Limewire” handwritten on the front of it. This CD-R was found in a brown CD case belonging to Larman.

Byers’s examination of C1H1 confirmed that a P2P program called Frostwire had been installed four months before the sharing incident and remained on the computer. Byers found music and a bestiality video in the Frostwire shared folder, but no child pornography. He also found files indicating that Limewire previously had been installed on C1H1. Most importantly, Byers found child pornography files with hash values matching those identified in the earlier sharing incident. C1H1’s temporary internet cache folder also contained data suggesting that child pornography previously had been accessed on that computer.²

The examination of TD-1 and TD-2 revealed more child pornography. Many of the images on TD-1 were “series” or “known file filter” images, meaning these images were of known victims previously identified by law enforcement. Again, several of these images matched the hash values of images identified in the sharing incident by the CPS software. Byers found that these child pornographic images were stored in a folder several levels down the “tree structure” of the device, meaning that the folders would have had to be consciously created by the user. Also contained on TD-1 were a large assortment of Larman’s personal photographs, including pictures of his tattoos and pictures of his wife. TD-2 contained fewer child pornographic images, although Byers was able to effectively identify three such images. The CD-R

² Once a computer views a webpage, “the computer automatically stores a copy of that webpage in a folder known as the cache.” *United States v. Moreland*, 665 F.3d 137, 142 (5th Cir. 2011). Whenever the computer user revisits that webpage, the presence of that file in the temporary internet cache allows the page to “load more quickly by retrieving the version stored in the cache.” *Id.* In this case, investigators could view the hash values of the files to see what images were viewed. Some of these images matched known child pornographic images.

No. 12-50855

Byers recovered contained several files with names that indicated the images were child pornography, although these images were not charged in Larman's indictment.

On April 4, 2012, a federal grand jury returned a four-count, superseding indictment charging Larman with violating 18 U.S.C. § 2252(a)(2) in Count One: Receipt of Child Pornography and Count Two: Attempted Distribution of Child Pornography, and 18 U.S.C. § 2252(a)(4)(B) in Counts Three and Four: Possession of Child Pornography. On April 16, 2012, Larman's jury trial began. Four days later, a jury found Larman guilty on all four counts. The district court judge later sentenced Larman to concurrent 188-month terms of imprisonment on Counts One and Two, and concurrent 120-month terms of imprisonment on Counts Three and Four. Larman appeals only Counts One, Two, and Three of his conviction. Thus, as far as the record shows, he stands convicted on Count Four.

II.

Larman's first issue on appeal challenges the sufficiency of the evidence used to support Counts One, Two, and Three of his child pornography conviction. Larman properly preserved this challenge by moving for a judgment of acquittal after the close of all evidence and thus the court's decision denying his motion for judgment of acquittal is reviewed *de novo*. *United States v. McDowell*, 498 F.3d 308, 312 (5th Cir. 2007). In reviewing the evidence, this court views it "in the light most favorable to the Government with all reasonable inferences to be made in support of the jury's verdict." *United States v. Moser*, 123 F.3d 813, 819 (5th Cir. 1997). The overarching question is whether "any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *United States v. Jara-Favela*, 686 F.3d 289, 301 (5th Cir. 2012) (quoting *Jackson v. Virginia*, 443 U.S. 307, 319 (1979)).

No. 12-50855

A.

Larman challenges the sufficiency of the evidence in Counts One and Three, in which he was found knowingly to have received and possessed child pornography, respectively. The direct evidence of knowing receipt in Count One was the testimony of Agents Marquez and Sletner that Larman had admitted to downloading child pornography on Limewire, a P2P program, approximately fifty times since June 2010. At trial, Larman consistently denied ever having told the agents that he downloaded child pornography on Limewire. Larman argues that the Government's reliance on the files contained within his temporary internet cache cannot form the sole basis of his receipt conviction because the Government failed to show that Larman "knowingly" received these images and that he exerted dominion and control over them.

Determining "[t]he weight and credibility of the evidence [is] the sole province of the jury." *United States v. Parker*, 505 F.3d 323, 331 (5th Cir. 2007). Here, the jury apparently found credible the agents' testimony that Larman admitted to the downloading of child pornography on Limewire and found not credible Larman's testimony that he made no such admission to the agents. Our court assesses the credibility of witness testimony only to the extent that it may be "incredible or patently unbelievable." *United States v. Lopez*, 74 F.3d 575, 578 (5th Cir. 1996). The agents' testimony is neither. On this evidence alone, Larman's conviction of receipt of child pornography on Count One can be affirmed.

The Government also presented circumstantial evidence that Larman received child pornography from the Internet. Hash values for several of the child pornographic images found on both C1H1 and TD-1 matched those that were shared via the P2P network on October 23, 2010. Although it was not charged, the CD-R containing child pornography was found in a brown CD case

No. 12-50855

that Larman admitted was his at trial. All of this evidence is enough, with respect to the receipt count, to support the jury's finding that the Government proved "the essential elements of the crime beyond a reasonable doubt." *Jara-Favela*, 686 F.3d at 301.

Larman also challenges his conviction in Count Three for possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(b). As evidence of Larman's knowing possession, the Government presented the files found on C1H1, TD-1, and TD-2. At trial, and at oral argument, Larman contended that the jury lacked a legal basis to find him guilty of possession of the illegal images under a constructive possession theory because his roommate, Benjamin Morgan, could have accessed, downloaded, and possessed the material himself rather than Larman.³ Possession, under this statute, may be either actual or constructive; actual possession "means the defendant knowingly has direct physical control over a thing at a given time." *United States v. Moreland*, 665 F.3d 137, 150 (5th Cir. 2011). Constructive possession, on the other hand, "is the ownership, dominion or control over an illegal item itself or dominion or control over the premises in which the item is found." *Id.*

Larman relies heavily on *Moreland* to argue that the Government was required to prove "something else (e.g., some circumstantial indicium of possession) . . . besides mere joint occupancy [to] support[] a plausible inference that the defendant had knowledge of and access to the . . . contraband." *Id.* Larman is correct when he asserts that where "a residence is jointly occupied, the mere fact that contraband is discovered at the residence will not, without more, provide evidence sufficient to support a conviction based upon constructive possession against any of the occupants." *Id.* Although evidence

³ Testimony at trial established that Larman's router, modem and WiFi connection were password protected. Morgan was the only other individual with the credentials to access Larman's network.

No. 12-50855

of mere occupancy is not enough, “additional evidence of the defendant’s knowing dominion or control of the contraband, besides the mere joint occupancy of the premises” can support a reasonable inference that the defendant had knowledge of and access to the child pornography. *Id.*

To be sure, the Government presented ample “additional evidence” of Larman’s knowing possession. Larman’s roommate, Morgan, testified that he did not know the two seized thumb drives existed. He further testified that he had never used Larman’s PlayStation 3 outside of the few occasions they played it together and that he had never used Larman’s desktop computer. Morgan described his knowledge of computer technology as being limited to surfing the Internet. Morgan was adamant that he had never seen or viewed child pornography. There was no evidence to suggest Morgan had ever used any of the media devices outside the presence of Larman. When Special Agent Byers ran a forensics check on Morgan’s personal laptop, he did not find any child pornography, P2P software, or cleanup software to suggest data had been deleted.

There is a notable dearth of evidence linking Morgan to use of any of the media containing child pornography. On the other hand, there is compelling evidence linking Larman to use of the media devices. First, Larman admitted that only he used those media devices, an admission he recanted at trial. Agent Byers testified that the file structure of C1H1 was intentionally configured to send and receive data through P2P software; law enforcement found P2P software on Larman’s computer, and Larman testified that he knew how to create, delete, and move files electronically. The presence of child pornography on Larman’s multiple media devices, along with the CD-R containing child pornography in Larman’s brown CD case, a case that Morgan testified he had never seen before, all constitute additional evidence necessary to support Larman’s conviction for possession on Count Three. For the reasons above, we

No. 12-50855

find the evidence sufficient to support Larman's convictions on Counts One and Three, that is for receipt and possession of child pornography, respectively.

B.

On Count Two of his conviction, the jury found that Larman attempted to distribute child pornography on October 23, 2010, when the CPS system indicated that a computer using his IP address was sharing child pornographic images. At trial, Larman contested the Government's assertion that he was the individual sharing the files. Larman's alibi was that he was on duty at the local army base from 9 a.m. until 9 p.m. on October 23. Larman argues that he could not have started sharing the files at 8:12 a.m. and stopped sharing them at 8:57 a.m. because he was not present at his house during this time. Although Larman appears to have been at work during this incident of sharing, the Government put on ample evidence that Larman did not need to be physically present at the house to allow the files' transmission to other computers.

The Government compared the act of sharing of files on a P2P network to the operation of a self-service gas station where the sharer merely provides access to the files and the recipient "helps himself" to the files by downloading them. *United States v. Richardson*, 713 F.3d 232, 236 (5th Cir. 2013) (citing *United States v. Shaffer*, 472 F.3d 1219, 1223-24 (10th Cir. 2007)). At oral argument, the Government cleared up any confusion regarding the duration of the sharing by explaining that the CPS system began pinging, or sending a signal to, P2P users' folders at 8:12 and ceased at 8:57; the sharing ceased because the CPS system quit searching, not because of some activity from Larman's IP address while Larman was at work.

The evidence supporting the attempted distribution count is circumstantial in nature, but it nevertheless paints a clear picture for the jury to determine that Larman was the culpable individual. Larman's modem was

No. 12-50855

password protected and, as previously discussed, there is no evidence that Morgan ever accessed Larman's media devices outside of his presence. The IP address sharing the child pornography on October 23 matched Larman's modem, and the subsequent investigation of Larman's computer revealed that many of the images found on it matched those made available on the P2P network during the sharing incident. Even though Larman's shared folder did not contain any child pornography at the moment it was seized, five months had passed since the sharing incident. The Government established that Larman possessed the technical expertise to create, delete, and manipulate folders and files on his computer; a rational trier of fact could conclude that if Larman used Frostwire to distribute the images, he likely moved them out of the shared folder. On the other hand, evidence that Limewire previously had been installed and then deleted from C1H1 also suggests that Larman could have used that particular P2P program to share the files and that its subsequent deletion before the execution of the search warrant prevented another shared folder from being examined.

In sum, we hold that there was sufficient evidence for the jury to convict Larman on Counts One (receipt), Two (attempted distribution), and Three (possession) of his child pornography conviction.

III.

Next, Larman raises an evidentiary issue and argues that the district court committed reversible error when it refused to allow him to testify as to his version of the incriminating statements he made to the agents in their interview with him, that is, unless such testimony was accompanied by a limiting instruction.

Under Rule 103(a) of the Federal Rules of Evidence, a party may only challenge a district court's evidentiary ruling excluding evidence if that party "informs the court of its substance by an offer of proof, unless the substance

No. 12-50855

was apparent from the context.” FED. R. EVID. 103(a). This court “will not even consider the propriety of the decision to exclude the evidence at issue, if no offer of proof was made at trial.” *United States v. Winkle*, 587 F.2d 705, 710 (5th Cir. 1979).

In response to the court’s exclusion of the testimony, Larman failed to offer the substance of the excluded testimony. When informed that Larman’s testimony would be subject to the limiting instruction, Larman’s attorney told the district court that he would not ask the question “at [that] point.” We understand that his testimony would have contradicted the agents’ account of what he told them, but what is not apparent from the record, is *how* it would have differed from the agents’ accounts.⁴ In short, counsel simply made no offer of proof. As a result, we find that Larman’s challenge to the district court’s exclusion of his testimony fails due to an insufficient offer of proof.

IV.

Finally, Larman challenges his conviction based on two alleged errors with the jury instructions. We review a district court’s decisions on jury instruction for abuse of discretion. *United States v. Demmitt*, 706 F.3d 665, 675 (5th Cir. 2013).

First, Larman challenges the district court’s deliberate ignorance instruction on grounds that the instruction is not supported by the facts of the case. Even if we assume error, we have consistently held that such an error is “harmless where there is substantial evidence of actual knowledge.” *United States v. Threadgill*, 172 F.3d 357, 369 (5th Cir. 1999) (citation and internal

⁴ Mere statements that a criminal defendant will give “his version” of a conversation are “not sufficient to make known to the court the substance of the evidence.” *United States v. Winkle*, 587 F.2d 705, 710 (5th Cir. 1979). Our precedent is clear that “[a] general description of the excluded evidence . . . [will] not preserve error.” *United States v. Ballis*, 28 F.3d 1399, 1406 (5th Cir. 1994).

No. 12-50855

quotation marks omitted). The overwhelming evidence, recounted in this opinion, of Larman's actual knowledge renders the error harmless.⁵

Second, Larman challenges the district court's refusal to give a *Pennington* instruction addressing Larman's knowledge of the illicit images on his media devices.⁶ The instruction derives from *United States v. Pennington*, in which two truck drivers were indicted on drug possession charges after authorities discovered large amounts of marijuana in their tractor-trailer. 20 F.3d 593 (5th Cir. 1994). Both defendants claimed they did not know the drugs were in the vehicle, and that they could not be guilty because the Government failed to produce evidence of such knowledge. *Id.* at 597-98. In response to their argument, this court declared that "[t]he knowledge element in a possession case can be inferred from control of the vehicle in some cases[,] but where the illicit substance is "hidden . . . control [over the vehicle] alone is not sufficient to prove knowledge." *Id.* at 598. Although we found that the marijuana in the defendants' tractor-trailer was indeed "hidden," we nevertheless upheld the verdict because the Government had offered additional evidence beyond the defendants' mere control of the vehicle, to show the defendants' guilt. *Id.*

Here, Larman's files were easily and quickly accessible. The fact that images found on TD-1 and TD-2 sat below the top level of visible folders is simply not enough for those images to be considered "hidden" within the

⁵ Here, the Government offered ample evidence that Larman had actual knowledge of his receipt, attempted distribution, and possession of child pornography. Such evidence included the agents' testimony regarding Larman's admissions, the structure of the file folders on C1H1, TD-1, and TD-2, along with Larman's ownership of the CD-R, which contained several child pornography images.

⁶ As an initial matter, we have no authority that a *Pennington* instruction is even appropriate in any child pornography case. In one unpublished decision only, have we evaluated a claim whether a *Pennington* instruction was proper involving child pornography possession. *United States v. Adams*, 338 F. App'x 417, 420 (5th Cir. 2009).

No. 12-50855

meaning of *Pennington*. We therefore find no abuse of discretion in refusing Larman's requested *Pennington* instruction.

V.

We now turn to Larman's sentencing claims. Larman's raises two issues, both involving sentencing enhancements. A "district court's application of the Guidelines . . . is reviewed *de novo*." *United States v. Smith*, 440 F.3d 704, 706 (5th Cir. 2006). We "accept[] findings of fact made in connection with sentencing unless clearly erroneous." *Id.*

Larman first challenges his two-level enhancement imposed under § 2G2.2(b)(3)(f), reflecting an enhancement based upon distribution of child pornography. Our earlier finding that the evidence supported the jury's verdict that Larman attempted to distribute child pornographic images—as charged in Count Two of the indictment—adequately supports the imposition of this enhancement without further discussion.

Larman's next challenge is to his two-level enhancement imposed under § 3A1.1(b)(1), on grounds that his victims were vulnerable victims. He argues that his specific offense guideline, under § 2G2.2(b)(2), already takes into account the ages of the children, and so the imposition of that particular vulnerable victim enhancement constitutes double counting. We rejected such an argument in a recent opinion. *See United States v. Jenkins*, 712 F.3d 209, 213-14 (5th Cir. 2013) (holding that an enhancement under § 3A1.1(b)(1) is still appropriate when the "under 12" enhancement in § 2G2.2(b)(2) is also applied). Thus, there is no error here.

VI.

In sum, we conclude, first, that there was sufficient evidence to convict Larman on Counts One (receipt), Two (attempted distribution), and Three (possession) of his indictment. Second, because Larman failed to make an offer of proof, he cannot challenge the district court's evidentiary ruling excluding

No. 12-50855

part of his testimony at trial. Third, any error concerning a deliberate ignorance instruction was harmless because of overwhelming evidence of Larman's actual knowledge. Fourth, the district court did not err in refusing Larman's *Pennington* instruction because the child pornography files were not "hidden" on his media devices. And, finally, both of the challenged sentencing enhancements were proper under the Guidelines. Accordingly, the judgment of the district court is

AFFIRMED.