IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

No. 17-11339

United States Court of Appeals
Fifth Circuit
FILED
August 15, 2019
Lyle W. Cayce
Clerk

UNITED STATES OF AMERICA,

Plaintiff–Appellee,

versus

DARYL GLENN PAWLAK,

Defendant–Appellant.

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

Before SMITH, WIENER, and ELROD, Circuit Judges.

JERRY E. SMITH, Circuit Judge:

Daryl Pawlak was convicted of receipt of child pornography and access with intent to view child pornography involving a prepubescent minor. Pawlak asserts that the district court erred in denying his motions to dismiss the indictment and to suppress evidence, that the evidence was insufficient to sustain his convictions on either count, and that the court clearly erred in applying

a two-level sentencing enhancement for obstruction of justice. Finding no error, we affirm.

I.

A.

In December 2014, federal law enforcement officials learned that a U.S.-based Internet protocol ("IP") address was hosting a website called "PlayPen," which contained a significant amount of child pornography. *United States v. Ganzer*, 922 F.3d 579, 581 (5th Cir. 2019), *petition for cert. filed* (July 23, 2019) (No. 19-5339). The website operated on an anonymity network and was accessible using publicly available software known as The Onion Router ("TOR"). *Id.*

Unlike the traditional Internet, TOR software anonymizes a user's actual IP address (which can be tied to a physical location) by routing the user's connection through a series of randomly selected computers on the network. *Id.* That feature generally makes it impossible for law enforcement officials to identify the administrators and users of websites containing child pornography, such as PlayPen, without employing other investigative techniques. *Id.*

In January 2015, the FBI executed a search warrant and obtained a copy of the server hosting the PlayPen website, which it transferred to a government-controlled facility in Virginia. *Id.* After obtaining a second warrant from a magistrate judge in the Eastern District of Virginia, *id.*, the FBI began a thirteen-day sting operation aimed at unmasking the identities of PlayPen users.[1]

[1] The government notes that although it "did operate the PlayPen site during this brief period of time, it took 'every possible effort to mitigate and prevent any additional physical abuse to children.'" Such efforts included "remov[ing] a portion of the website that encouraged members to produce and post new child pornography."

The operation centered on the use of specialized malware called the Network Investigative Technique ("NIT"). *Id.* "The NIT was a form of malware that augmented the content sent by Playpen to the computers of Playpen users with directions instructing those computers to send identifying information to a computer controlled by the government," *id.*, including "the computer's IP address and when the NIT determined [it]; a unique identifier for the computer generated by the NIT; the type of operating system used by the computer and the operating system's active username . . . ; the computer's host name; and the computer's media access control," *id.* at 581–82. The government further explains that

> [t]he NIT would not deploy onto a PlayPen user's computer until that individual logged into the website (which required them to have the TOR browser, know the 16-character website address,[2] and enter their login information for PlayPen), accessed a certain section in the site, and then actually requested content by clicking on a post in one of the more egregious sections.

B.

Using the NIT, federal agents linked PlayPen user "notsoslow"—later determined to be Daryl Pawlak—with an IP address associated with a residence in Johnson County, Texas. The user had been logged into PlayPen for more than fourteen hours before the NIT deployed on his computer in March 2015, and he had spent an additional hour-and-a-half on PlayPen during the FBI's operation of the website. The NIT also returned Pawlak's computer username ("d.pawlak"), the name of the computer ("Sigma94"), and the computer's MAC address.

On October 1, 2015, after obtaining a search warrant for Pawlak's residence, FBI agents interviewed Pawlak's wife. Using the wife's cell phone,

---

[2] The website address was comprised of "a randomly generated stream of [sixteen] characters ending in '.onion.'"

Agent Marya Wilkerson called Pawlak and recorded the conversation. On the call, Pawlak admitted, *inter alia*, that he had downloaded and viewed child pornography using laptops from two different employers, had an email address utilizing the term "notsoslow," had previously used a work computer with the name of "Sigma94," and believed his username on that computer was "d.pawlak." Pawlak also acknowledged that the computer (the "Sigma94 computer") had been in his possession from October 2014 until May 2015, when he returned it to his former employer, Sigma Cubed following his termination.

In the recorded conversation, Pawlak stated that he had initially viewed child pornography approximately three or four years earlier while working for a previous employer. He admitted that he preferred child pornography involving prepubescent females approximately seven to eleven years old, that he often accessed such pornography on a website called "Girls Hub," and that he had last viewed child pornography about one week before.

Later that day, Pawlak and Agent Wilkerson engaged in a second conversation that was not recorded. Pawlak admitted that he had attempted to delete the contents of the hard drive on his current work computer (the "Independence Oil computer") but was unable to do so.

The FBI later acquired the Sigma94 computer from Sigma Cubed. Pawlak was the first and only employee to use the computer, which had remained in a sealed box in Sigma Cubed's offices after he returned it in May 2015. Following a forensic examination, law enforcement officials discovered several images of child pornography in the temporary Internet cache of the Sigma94 computer. The presence of the images in the cache demonstrated that the files came from the Internet, as well as that they were received and stored on the computer. Federal agents also found evidence of seven other images of child pornography on the computer.

In addition, federal agents captured information from when Pawlak accessed the PlayPen website both before and during the thirteen days it was operated by the government. Evidence showed that Pawlak clicked on several posts containing child pornography involving prepubescent female children.

In October 2015, the FBI obtained access to the Independence Oil computer, on which investigators discovered approximately eight hundred images and four videos of child pornography. Pawlak was charged with receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2)(A) (Count One), and access with intent to view child pornography involving a prepubescent minor, in violation of 18 U.S.C. § 2252A(a)(5)(B) (Count Two).

Pawlak moved to suppress the evidence obtained using the NIT, as well as all other evidence discovered as a result of its deployment. He claimed that the warrant was void *ab initio* because it violated the scope of the issuing magistrate judge's authority under Federal Rule of Criminal Procedure 41(b). He also moved to dismiss the indictment against him asserting that the government's operation of the PlayPen website constituted outrageous conduct. The district court denied both motions.

Following a three-day trial, a jury convicted Pawlak on both counts. At sentencing, the presentence report recommended a two-level obstruction-of-justice enhancement relating to Pawlak's attempt to delete the contents of the hard drive on his Independence Oil computer. The district court overruled Pawlak's objection to the enhancement. The court sentenced Pawlak to 210 months' imprisonment on each count, to be served concurrently, followed by a supervised release term of fifteen years.

Pawlak raises five issues on appeal. First, he asserts that the district court erred in denying his motion to dismiss the indictment based on outrageous government conduct. Second, Pawlak avers that the court erred in

denying his motion to suppress. Third, he contends that the evidence was insufficient to sustain his conviction for access with intent to view child pornography involving a prepubescent minor (Count Two). Fourth, Pawlak maintains that the evidence was insufficient to support a conviction for receipt of child pornography (Count One). Fifth, Pawlak claims that the district court clearly erred by applying the U.S.S.G. § 3C1.1 obstruction-of-justice enhancement.

II.

Pawlak avers that the district court erred in denying his motion to dismiss. "[W]e review *de novo* whether outrageous conduct requires dismissal of an indictment." *United States v. Sandlin*, 589 F.3d 749, 758 (5th Cir. 2009).

A.

"The due process clause protects defendants against outrageous conduct by law enforcement agents." *United States v. Arteaga*, 807 F.2d 424, 426 (5th Cir. 1986). However, "[g]overnment misconduct does not mandate dismissal of an indictment unless it is so outrageous that it violates the principle of fundamental fairness under the due process clause of the Fifth Amendment." *Sandlin*, 589 F.3d at 758–59 (citation omitted). Consequently, "the outrageous-conduct defense requires not only government overinvolvement in the charged crime but a passive role by the defendant as well. A defendant who actively participates in the crime may not avail himself of the defense." *Arteaga*, 807 F.2d at 427.

We evaluate the government's conduct "in light of the undercover activity necessary to the enforcement of the criminal laws." *United States v. Fortna*, 796 F.2d 724, 735 (5th Cir. 1986) (citation omitted). The outrageous-conduct standard is "extremely demanding," *Sandlin*, 589 F.3d at 758, and "a due process violation will be found only in the rarest and most outrageous circumstances," *Arteaga*, 807 F.2d at 426 (citation omitted).

B.

Pawlak asserts that, for three reasons, the district court erred in denying the motion to dismiss. First, he contends that he was a mere passive participant in the enterprise because "there is no evidence that [he] posted to any forums, communicated with others on the [PlayPen] site, shared information, or in any way produced or uploaded any materials." In doing so, Pawlak attempts to distinguish *United States v. Venson*, 82 F. App'x 330, 332–33 (5th Cir. 2003) (per curiam), in which we rejected an outrageous-conduct defense in a case involving child pornography.

Second, Pawlak maintains that, by operating the PlayPen website, the government aided in the public distribution of child pornography. Therefore, in addition to offending standards of fairness and decency, the government violated federal law.

Third, Pawlak states that the government's actions ignored its internal policies concerning the investigation of Internet crimes because "the FBI took no measures whatsoever to control the replication and distribution of pictures and videos from its undercover website." He also asserts that the government's actions in this case "resulted in the continued victimization of countless innocent children." Consequently, Pawlak contends that because he was a mere passive participant, and the government's overinvolved conduct was outrageous, the court erred in denying the motion to dismiss.

In response, the government maintains that "[t]he district court correctly denied Pawlak's motion to dismiss based on alleged outrageous government conduct given his willing and active participation in the offense." It offers two arguments in support of that position.

First, the government emphasizes that a defendant who actively partakes in a crime cannot avail himself of the outrageous-conduct defense.

Consequently, because Pawlak was "an active, willing, and predisposed child-pornography consumer," he is not entitled to assert that defense. The government points to several Fifth Circuit precedents where, despite an active role played by the government, we rejected the assertion of the outrageous-conduct defense because of the defendant's willing participation.[3]

Pawlak actively viewed child pornography for several years before the FBI's investigation. Before the government's operation of the PlayPen website, Pawlak spent nearly fourteen hours, over a six-month period, logged into the site. Moreover, he continued to seek out such material even after the FBI's PlayPen operation ended. Therefore, the government maintains, the outrageous-conduct defense is not available.

Second, the government emphasizes that we have never invalidated a conviction based on the assertion of that defense. It also notes that we seemingly defined the outer limits of permissible government conduct in *United States v. Tobias*, 662 F.2d 381 (5th Cir. Unit B Nov. 1981).

In *Tobias*, the DEA established a fake chemical-supply company and "placed an advertisement offering over-the-counter sales of chemicals and laboratory equipment." *Id.* at 383. The defendant in that case, Thomas Tobias, placed an order for various chemicals to manufacture cocaine. *Id.* Tobias later tried to cancel the order by telephoning an undercover DEA agent after he determined that cocaine would be too difficult to manufacture. *Id.* Pretending to be sympathetic, the agent suggested that Tobias manufacture phencyclidine ("PCP"). *Id.* at 383–84. Tobias then asked the agent to send him the chemicals necessary to make PCP. *Id.* at 384. After receiving the chemicals and formula

[3] *See United States v. Ivey*, 949 F.2d 759, 769 (5th Cir. 1991); *United States v. Evans*, 941 F.2d 267, 270–71 (5th Cir. 1991) (per curiam); *United States v. Yater*, 756 F.2d 1058, 1066 (5th Cir. 1985).

for PCP, Tobias made more than a dozen calls to the fictitious company for assistance with manufacturing. *Id.* The DEA eventually obtained a warrant and found liquid PCP at Tobias's residence. *Id.*

We rejected Tobias's assertion of the outrageous-conduct defense, finding that he "was a predisposed active participant, motivated solely by a desire to make money." *Id.* at 387. We stressed "that government infiltration of criminal activity is a recognized and permissible means of investigation." *Id.* at 386 (internal quotation marks and citation omitted). Consequently, no due process violation occurred. *See id.* at 387. Nonetheless, we cautioned that the "case does set the outer limits to which the government may go in the quest to ferret out and prosecute crimes in this circuit." *Id.*

Against this backdrop, the government maintains that the FBI's brief sting operation involving the PlayPen website falls well short of the boundaries established in *Tobias*. It notes that "[t]he FBI . . . did not create PlayPen, and . . . it did not alter the site's functionality, add additional child pornography, or actively solicit new users. Rather, the government simply maintained the preexisting structure that Playpen website visitors allegedly used to distribute and receive child pornography among themselves." Accordingly, the government contends it was significantly less active than in *Tobias* because it "only took over an existing site and did not solicit new members." It therefore urges us to affirm the denial of Pawlak's motion to dismiss.[4]

Pawlak fails to establish either prong associated with the outrageous-conduct defense. Concerning the requirement that the defendant play a passive role, the evidence demonstrates that Pawlak was an active consumer of child pornography both before and after the FBI's sting operation. Moreover,

[4] The government stresses that every district court to consider the outrageous-conduct defense in the context of the FBI's operation of the PlayPen website has rejected it.

to access the PlayPen website, a user was required to obtain specialized software, enter a specific sixteen-character website address, and log in using a unique username and password. Because Pawlak was an active participant in the crime, he is not entitled to assert the outrageous-conduct defense on that ground alone. *See Arteaga*, 807 F.2d at 427.

Furthermore, the government's conduct was not outrageous and did not violate fundamental fairness. Viewing the sting operation "in light of the undercover activity necessary to the enforcement of the criminal laws," *Fortna*, 796 F.2d at 735 (citation omitted), the government's conduct does not run afoul of the Fifth Amendment. Here, the FBI received judicial approval to operate the PlayPen site, and it did so for only thirteen days. During that time, the FBI sought to mitigate the further exploitation of children by removing the portion of the site that encouraged members to produce and upload new images of child pornography.

Ultimately, the sting operation successfully targeted a hidden website where thousands of users were viewing a significant amount of child pornography in a nearly untraceable manner. The operation also rescued hundreds of children, including dozens in the United States, from sexual abusers. Therefore, the district court did not err in denying the motion to dismiss.

III.

Pawlak next claims that the district court erred in denying his motion to suppress. "We review the denial of a motion to suppress in the light most favorable to the prevailing party." *United States v. Hernandez*, 670 F.3d 616, 620 (5th Cir. 2012). "The district court's factual findings are reviewed for clear error, and its legal conclusions are reviewed *de novo*." *Id.* "A finding of fact is clearly erroneous if we are left with a definite and firm conviction that a mistake has been committed." *Id.* (internal quotation marks and citation omitted).

"We uphold a district court's denial of a suppression motion if there is any reasonable view of the evidence to support it." *United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018) (internal quotation marks and citation omitted).

A.

"The fact that a Fourth Amendment violation occurred—*i.e.,* that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). The Supreme Court has "repeatedly rejected the argument that exclusion is a necessary consequence of a Fourth Amendment violation." *Id.* at 141. Accordingly, "[w]hen police act under a warrant that is invalid for lack of probable cause," *id.* at 142, "evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant typically should not be excluded." *Contreras*, 905 F.3d at 857 (internal quotation marks and citation omitted). Moreover, "a warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *United States v. Leon*, 468 U.S. 897, 922 (1984) (internal quotation marks and citation omitted).

Nonetheless, there are four circumstances in which an "officer's reliance on the magistrate's probable-cause determination and on the technical sufficiency of the warrant he issues" is not objectively reasonable. *United States v. Cherna*, 184 F.3d 403, 407 (5th Cir. 1999) (citation omitted). First, "if the magistrate or judge . . . was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth." *Leon*, 468 U.S. at 923. Second, if the "magistrate wholly abandoned his [neutral and detached] judicial role." *Id.* Third, if the "officer . . . rel[ied] on a warrant [that was] based on an affidavit so lacking in

indicia of probable cause as to render official belief in its existence entirely unreasonable." *Id.* (internal quotation marks and citation omitted). And fourth, if the warrant was "so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Id.*

"We employ a two-step process for reviewing a district court's denial of a motion to suppress when a search warrant is involved." *Cherna*, 184 F.3d at 407. First, we analyze "whether the good-faith exception to the exclusionary rule" applies. *Id.* If the exception does apply, we affirm the denial of the motion to suppress. *Id.* If it does not, we review whether "the magistrate had a substantial basis for" determining that probable cause existed. *Id.* (citation omitted).

B.

Pawlak raises three arguments in support of his contention that the district court erred in denying his motion to suppress. First, he asserts that the court erred when it declined to require the testimony of Agent McFarlane, the affiant for the NIT warrant application, concerning McFarlane's subjective intent. Second, Pawlak maintains that the court erroneously concluded that the subjective intent of government officials was irrelevant because other courts later found the warrant to be valid.

Third, Pawlak avers that the district court erred because the officers' reliance on the warrant was not objectively reasonable. Pawlak contends that *In re Warrant*, 958 F. Supp. 2d 753 (S.D. Tex. 2013), "put the government on notice that using a warrant issued by a Magistrate Judge in one district to execute malware searches in another is not legal." Consequently, because the government "was fully aware at least two years before it sought the NIT Warrant . . . that [Federal Rule of Criminal Procedure] 41 did not permit

multi-district computer hacking," its agents' reliance on the warrant was not objectively reasonable.

The government responds that Pawlak's focus on "the subjective intent of the officers who secured the NIT Warrant" is misplaced. It asserts that the "good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances" (quoting *Herring*, 555 U.S. at 145). The government also avers that we may "not attempt an expedition into the minds of police officers to determine their subjective belief regarding the validity of the warrant" (quoting *United States v. Payne*, 341 F.3d 393, 400 (5th Cir. 2003)). Consequently, because "Pawlak does not point to any of the *Leon* factors that would suggest the officers failed to act in good faith," the government posits that his "argument should fail."

Moreover, although the district court found that the magistrate judge who initially issued the NIT warrant exceeded the scope of her authority, it also highlighted that several other district courts had reached the opposite conclusion. Therefore, because the matter represented a close legal question, the government contends that it "did not act improperly in seeking th[e] warrant." The government also stresses that because the officers deploying the NIT had no reason to know that the magistrate judge had erred, their reliance on the warrant was objectively reasonable.

Lastly, the government carefully distinguishes this case from *In re Warrant*. It emphasizes that "the information sought to be seized in *In re Warrant* was considerably more extensive and intrusive than the identifying information sought in this case," and it underscores that "a single decision from a magistrate judge in a dissimilar case did not give the government the unambiguous knowledge that such warrants were impermissible." Moreover, "that authori-

ties believed clarification of Rule 41(b) would be helpful does not somehow prove that they knew the NIT Warrant could not validly issue under the circumstances of this case."

Our recent decision in *Ganzer* effectively compels the conclusion that the district court did not err in denying Pawlak's motion to suppress. In that case, we found that the good-faith exception applied to evidence seized because of the NIT warrant, even assuming that the magistrate judge in the Eastern District of Virginia exceeded the scope of her authority. *Ganzer*, 922 F.3d at 587–90. Moreover, we declined to "construe the government's efforts to have Rule 41(b) amended to specifically allow for warrants like the NIT warrant as an admission that such warrants were not previously allowed, but rather as an attempt to clarify an existing law's application to new circumstances." *Id.* at 589.

This case presents factual issues similar to those in *Ganzer*. Consequently, because here, as there, "law enforcement officials involved in the issuance and execution of the NIT warrant acted with an objectively reasonable good-faith belief that their conduct was lawful," *id.* at 590 (internal quotation marks, alteration, and citation omitted), the district court did not err in denying Pawlak's motion. Such a "conclusion is consistent with the holdings of each of our sister circuits to have considered challenges to the NIT warrant." *Id.*[5]

IV.

Pawlak contends that the evidence was insufficient on both counts. We

[5] *See United States v. Moorehead*, 912 F.3d 963, 970–71 (6th Cir. 2019); *United States v. Kienast*, 907 F.3d 522, 528–29 (7th Cir. 2018); *United States v. Henderson*, 906 F.3d 1109, 1119–20 (9th Cir. 2018); *United States v. Werdene*, 883 F.3d 204, 217–18 (3d Cir. 2018); *United States v. McLamb*, 880 F.3d 685, 690–91 (4th Cir. 2018); *United States v. Levin*, 874 F.3d 316, 322–24 (1st Cir. 2017); *United States v. Horton*, 863 F.3d 1041, 1051–52 (8th Cir. 2017); *United States v. Workman*, 863 F.3d 1313, 1317–21 (10th Cir. 2017).

review *de novo* Pawlak's sufficiency claims because he properly preserved the issues by moving for a judgment of acquittal during trial. *United States v. Moreland*, 665 F.3d 137, 148 (5th Cir. 2011). "In deciding whether the evidence was sufficient, we review all evidence in the light most favorable to the verdict to determine whether 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. Shum*, 496 F.3d 390, 391 (5th Cir. 2007).

A.

Although the government has broad authority to proscribe child pornography, this authority is not unlimited. *United States v. Williams*, 553 U.S. 285, 289 (2008); *see also Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 251–58 (2002). In *Free Speech Coalition*, the Court found that a federal statute banning "the possession and distribution of any visual depiction that is, or appears to be, of a minor engaging in sexually explicit conduct, even if it contained only youthful-looking adult actors or virtual images of children generated by a computer," *Williams*, 553 U.S. at 289 (internal quotation marks and citation omitted), was "overbroad and unconstitutional," *Free Speech Coal.*, 535 U.S. at 258.

The government notes that following *Free Speech Coalition*, defendants in this circuit have challenged their child-pornography convictions by contending "that the government failed to prove the children depicted in the pornography were real, as opposed to 'virtual,' children." We have rejected such a defense, concluding that "*Free Speech Coalition* did not establish a broad requirement that the Government must present expert testimony to establish that the unlawful image depicts a real child." *United States v. Slanina*, 359 F.3d 356, 357 (5th Cir. 2004) (per curiam). "The district court, as the trier of fact . . . , was capable of reviewing the evidence to determine whether the

Government met its burden to show that the images depicted real children." *Id.* Moreover, "[j]uries are still capable of distinguishing between real and virtual images." *Id.* (citation omitted).

B.

Count Two charged Pawlak with access with intent to view child pornography involving a prepubescent minor in violation of 18 U.S.C. § 2252A(a)(5)(B). Pawlak contends that "there was no evidence presented that the representations of children in the images accessed . . . were actual, real children," as opposed to "computer generated or morphed images." Consequently, because "the court's charge only allowed for the conviction upon a finding of child pornography that were images of real or actual children," the evidence introduced "was not sufficient to satisfy the elements of this offense."

The government counters with three points. First, it highlights that we have stated that images of child pornography are themselves sufficient to establish that actual children are depicted. In *United States v. McNealy*, 625 F.3d 858, 865–66 (5th Cir. 2010), a defendant asserted that the factfinder was incapable of ascertaining whether the charged images showed actual children. A government witness testified that he believed that the children depicted in the images were "real minors," *id.* at 865, but "conceded that he did not 'have the ability to look at these images and tell th[e] jury if they'[d] been altered or not,'" *id.*

On appeal, the defendant maintained that the government had failed to satisfy its burden of showing that the images were real. *Id.* We rejected that contention, concluding that "[n]othing in the record, including the images themselves, suggests that they are anything other than images of actual prepubescent children and young teenage girls engaged in what [the defendant] concedes is lewd and lascivious conduct." *Id.* at 866–67. We also highlighted

that "there is no evidence in the record before us that the state of technology is such that images of this nature could have been generated using virtual children." *Id.* at 867. Consequently, "[w]hile it remains the Government's burden to show that actual children were depicted, the images themselves sufficed to authenticate them in this regard." *Id.*

The government also points to testimony from Agent Wilkerson establishing "that *all* of the images the jury had seen to that point, including the Count Two images, and all other images at issue in the investigation of Pawlak, depicted real children." Another government official, Special Agent Daniel Alfin, answered "yes" when asked whether the Count Two images "'appear[ed] to' be real children."

Ultimately, viewing the evidence in the light most favorable to the verdict, the evidence was sufficient to sustain Pawlak's conviction on Count Two. Here, as was the case in *McNealy*, Pawlak points to no evidence in the record demonstrating that the Count Two images were anything other than what the government contended they were: child pornography involving actual prepubescent children. *See id.* at 866–67. Additionally, though it was "the [g]overnment's burden to show that actual children were depicted," here, as in *McNealy*, "the images themselves sufficed to authenticate them in this regard." *Id.* at 867. Consequently, this evidence, coupled with the testimony of Wilkerson and Alfin, was sufficient to support the verdict on this count.

C.

Count One charged Pawlak with receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A). Pawlak notes that the three images serving as the basis for Count One "were thumbnails found in the temporary internet files, cache location on the Sigma94 computer." Pawlak therefore contends that "[t]he problem with the sufficiency of evidence for these images . . . is that

the government has presented insufficient evidence to show where these items came from; when they were put on the computer; and who actually put the items on the computer."

Pawlak remarks that although he retained possession of the Sigma94 computer while employed by Sigma Cubed, "other employees had access to this computer for extended periods." Moreover, Pawlak acknowledges that he "made some admissions in a telephone conversation with Special Agent Wilkerson," but avers that "this conversation never established that he . . . viewed images on the Playpen website." Consequently, he asserts that because "[t]he government did not present evidence that these specific images were knowingly downloaded or received by Pawlak," the evidence was insufficient to sustain a conviction on this count.

Conversely, the government maintains that Pawlak's confession "to being a long-time consumer of child pornography, . . . a PlayPen member, and . . . particularly interested in images . . . involving prepubescent female children," coupled with the extensive forensic evidence tying him to the images, was sufficient to establish that he knowingly received the images. The government cites two precedents from this circuit in support of its position. In *United States v. Winkler*, 639 F.3d 692, 693 (5th Cir. 2011), we affirmed a defendant's conviction for knowing receipt of child pornography based on images found in his temporary Internet cache. We determined that "[t]he mere presence of the files in the cache is certainly proof that the files were *received*," *id.* at 699 (citation omitted), and we noted that the "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," *id.* Ultimately, we concluded that other evidence introduced by the government established "a pattern of child pornography receipt and possession that could also have caused a rational jury to conclude that [the defendant] knowingly

received the files." *Id.*

Moreover, in *United States v. Larman*, 547 F. App'x 475 (5th Cir. 2013) (per curiam), we affirmed a conviction for receipt of child pornography where images were found in the defendant's temporary Internet cache and he admitted to federal agents that he had downloaded child pornography. *Id.* at 479–81. The government stresses that—similar to the defendant in *Larman*—"Pawlak confessed to a longstanding interest in and consumption of child pornography." As part of his confession—which the government played at trial—"Pawlak indicated he spent approximately half an hour per week consuming child pornography and admitted to accessing it on internet sites." He "also admitted to having the username 'notsoslow' on the PlayPen website and to having a computer named 'Sigma94' with a username of 'd.pawlak' while working at Sigma Cubed, tying him to the computer which downloaded the images."

The government contends that "[l]ike the defendant in *Winkler*, the evidence showed Pawlak was a member of a website dedicated to child pornography and that he consumed a great deal of other child pornography, evincing a pattern of child-pornography receipt." Moreover, "like the defendant in *Larman*, Pawlak *confessed* to obtaining child pornography over the internet."

Ultimately, the evidence was more than sufficient to sustain the conviction on Count One. Images of child pornography were found on Pawlak's computer in his temporary Internet cache. Pawlak admitted, in a recorded conversation, to be being a long-time consumer of child pornography, and he was a member of PlayPen, a website dedicated to child pornography. Accordingly, viewed in the light most favorable to the verdict, this evidence sufficed to establish Pawlak's knowing receipt of child pornography.

V.

Pawlak maintains that the district court clearly erred in applying the obstruction enhancement. Because Pawlak specifically objected, we review the "district court's interpretation or application of the Sentencing Guidelines" *de novo*. *United States v. Adam*, 296 F.3d 327, 334 (5th Cir. 2002). We review the court's factual findings, including a finding of obstruction of justice, for clear error. *Id*. "Where a factual finding is plausible in light of the record as a whole, it is not clearly erroneous. Unless left with the definite and firm conviction that a mistake has been committed, [we] will not deem the district court's finding to be clearly erroneous." *Id*. (internal quotation marks and citation omitted).

A.

Section 3C1.1 of the U.S. Sentencing Guidelines, a sentencing adjustment for obstructing or impeding the administration of justice, provides that

> [i]f (1) the defendant willfully obstructed or impeded, or attempted to obstruct or impede, the administration of justice with respect to the investigation, prosecution, or sentencing of the instant offense of conviction, and (2) the obstructive conduct related to (A) the defendant's offense of conviction and any relevant conduct; or (B) a closely related offense, increase the offense level by 2 levels.

The application notes to the obstruction enhancement emphasize that, *inter alia*, "destroying or concealing . . . evidence that is material to an official investigation or judicial proceeding (*e.g.*, shredding a document or destroying ledgers upon learning that an official investigation has commenced or is about to commence), or attempting to do so" qualifies as "the type[] of conduct to which this adjustment applies." U.S.S.G. § 3C1.1 cmt. n.4(D).

B.

Pawlak avers that, for two reasons, the district court clearly erred in applying the obstruction enhancement. First, as Pawlak reads it, application

note 4(D) supports his position that his conduct does not amount to obstruction of justice because the attempt to erase his hard drive occurred contemporaneously with his arrest. *See id*. (stating an exception, under some circumstances, for conduct that "occurred contemporaneously with arrest" and was not "a material hindrance" to the investigation). Second, Pawlak contends that the mere act of searching for and downloading software designed to wipe a computer hard drive, without deploying it, does not constitute obstruction of justice. Consequently, because "he did not actually deploy the program and his conduct did not materially hinder the investigation and prosecution of the case," the court clearly erred.

In response, the government asserts that "[t]he district court did not clearly err in enhancing Pawlak's offense level for obstruction of justice because the evidence, including his confession, established that he downloaded a program meant to erase a computer hard drive containing a cache of child pornography." The government highlights that "after the FBI commenced its search-warrant execution . . . Pawlak searched for a program meant to wipe his hard drive." Pawlak later admitted to an FBI agent that he was unable to execute the program because he lacked an external drive necessary to utilize it. After examining the Independence Oil computer, a forensic computer expert confirmed that the software had been downloaded and installed on the same morning that the FBI executed a search warrant at Pawlak's residence. The government therefore contends that Pawlak fails "to show any error, much less clear error, in the district court's application of the obstruction enhancement based upon the concrete steps he took towards deleting material evidence from his computer after his conversation with" the FBI agent executing the search warrant.

The court did not clearly err in applying the obstruction enhancement. The evidence demonstrates, and Pawlak readily admits, that he took affirma-

tive steps to download a program aimed at permanently deleting the contents of the Independence Oil computer hard drive, including more than eight hundred images and four videos of child pornography. The successful deployment of that program would have deleted material evidence from the hard drive, thereby hindering the investigation. *See* U.S.S.G. § 3C1.1 cmt. n.4(D). That Pawlak was ultimately unsuccessful in deploying it is irrelevant: A defendant also qualifies for the enhancement when he merely attempts to obstruct justice. *Id.* § 3C1.1; *see also id.* § 3C1.1 cmt. n.4(D).

Moreover, Pawlak's attempt to obstruct justice was not contemporaneous with his arrest. Instead, he attempted to wipe his hard drive shortly after he learned that federal agents were searching his house. *Cf. id.* § 3C1.1 cmt. n.4(D). Consequently, the district court did not clearly err in applying the two-level obstruction enhancement.

AFFIRMED.