NOT RECOMMENDED FOR PUBLICATION
File Name: 20a0150n.06

No. 19-5686

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

FILED
Mar 13, 2020
DEBORAH S. HUNT, Clerk

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. DENNIS AMMONS, Defendant-Appellant.	)	ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF KENTUCKY

Before: MERRITT, THAPAR, and LARSEN, Circuit Judges.

LARSEN, Circuit Judge. A jury convicted Dennis Ammons of knowingly accessing child pornography with intent to view it. The district court sentenced him to 110 months in prison. On appeal, Ammons challenges both his conviction and his sentence. We AFFIRM.

I.

In 2014, the FBI began investigating a website known as "Playpen." Playpen was an online forum that advertised and distributed child pornography. Once logged in, users could view an extensive collection of pictures and videos containing child pornography.

Playpen was not accessible through traditional internet browsers. Instead, the site could only be accessed through what is colloquially referred to as the "dark web." *See United States v. Tagg*, 886 F.3d 579, 582 (6th Cir. 2018). Users had to download special software known as "The Onion Router" or "Tor," which allowed them to anonymously access a network of hidden websites. Through the Tor software, users then had to input an intricate web address consisting of random, algorithm-generated characters to reach Playpen's site. This web address was not linked

to traditional search engines like Google; it had to be obtained through other means, such as direct communication with pre-existing users.

With help from a foreign government, the FBI located a server containing a copy of Playpen's website. In January of 2015, agents obtained a search warrant and seized a copy of that server. Agents then identified and apprehended Playpen's administrator the following month. At that point, the FBI assumed control over Playpen. But even having control did not allow the FBI to identify the website's users; the Tor software masked their IP addresses.

The government sought a warrant from a magistrate judge in the Eastern District of Virginia—where the FBI had transported Playpen's server—to deploy what is known as a "Network Investigative Technique" (NIT). An NIT is a form of "government-created malware." *United States v. Werdene*, 883 F.3d 204, 206 (3d Cir. 2018). It unmasks a user's IP address by embedding instructions within the website's code that force the user's computer to transmit its IP address to a government-controlled server. The magistrate judge issued the warrant on February 20, 2015 (the Virginia Warrant).

Using the NIT, the government obtained an IP address associated with the username "H8RL3Y." This user had accessed several child-pornography images on Playpen over a six-hour period in early March 2015. The user had also responded to a post titled "Pthc 14Y Lil Zinaida 13Y Boy (51.15)," asking "What's the password?" The post contained a link to an external website where visitors could download child pornography.

The FBI ultimately traced H8RL3Y's IP address to a home in Muldraugh, Kentucky, where Ammons lived with his sister and her two minor children. The government sought and obtained a warrant to physically search Ammons' residence for evidence of child pornography (the Kentucky Warrant). The application for the Kentucky Warrant relied on the information obtained through

the NIT to establish probable cause. The subsequent search and seizure of Ammons' computer revealed 220 child-pornography images (113 non-duplicates) stored in the cache of his Chrome web-browser. The metadata attached to these images indicated that they had been accessed on October 22, 2015.

Following the search, the FBI interviewed Ammons. He waived his *Miranda* rights and agreed to answer the agents' questions. Ammons told the agents that he was the primary user of the computer in his household. He also explained that he had installed a password protected wireless router in the house a few months earlier. Finally, after initially denying ever seeing child pornography, Ammons admitted that he came across child pornography while exploring the "dark web." He named multiple sites where he had seen child pornography and described the images to the agents—though he claimed he was not a "collector" of these images.

The FBI also interviewed Ammons' 16-year-old niece, who lived in his Kentucky home. She told agents that Ammons had previously taken nude photographs of her. She described an incident in which Ammons had caught her taking nude pictures of herself. She stated that Ammons confronted her, confiscated the phone on which she had taken the pictures, and threatened to tell her mother unless she agreed to pose nude for Ammons. She claimed that Ammons then took nude photographs of her, forcing her to pose with her legs spread apart exposing her genitals. These photographs were never found.

A grand jury indicted Ammons on two counts: (1) production of child pornography, in violation 18 U.S.C. § 2251(a) and (e); and (2) knowingly accessing child pornography with intent to view it, in violation of 18 U.S.C. § 2252A(a)(5)(B). Prior to trial, Ammons moved to suppress the evidence obtained from his computer through both the NIT and the physical search of his home. He argued that the Virginia Warrant was invalid because the issuing magistrate judge lacked

jurisdiction over Kentucky, where Ammons' computer was located when the government implemented the NIT. Because the subsequent Kentucky Warrant was obtained with information from the NIT, Ammons contended that evidence from both searches must be suppressed. The district court denied Ammons' motion, and the case proceeded to trial.

After trial, the jury rendered a split verdict, acquitting Ammons of producing child pornography but convicting him of knowingly accessing child pornography with intent to view it. Ammons moved for a judgment of acquittal, arguing that the evidence was insufficient to support his conviction. The district court denied his motion.

Ammons' conviction carried a maximum prison sentence of ten years. *See* 18 U.S.C. § 2252A(b)(2). At sentencing, the district court concluded that the appropriate Guidelines range was 108 to 120 months. Ammons argued that his Guidelines range was unreasonable. Specifically, he contended that the enhancements contained in U.S.S.G. § 2G2.2 resulted in nearly all child-pornography offenders receiving the maximum sentence; as a result, Ammons argued, the court should ignore those enhancements and issue a below-Guidelines sentence. The district court disagreed, sentencing Ammons to 110 months in prison—10 months shy of the statutory maximum. Ammons appealed.

II.

A.

Ammons argues first that the district court erred by denying his motion to suppress. Evidence obtained in violation of the Fourth Amendment may be subject to suppression at trial. *See United States v. Fisher*, 745 F.3d 200, 203 (6th Cir. 2014). But not all Fourth Amendment violations result in suppression. *Id.* The exclusionary rule's "sole purpose" is to deter Fourth Amendment violations. *See Davis v. United States*, 564 U.S. 229, 236 (2011). Thus, when officers

"conduct a search in objectively reasonable reliance on a warrant later held invalid," the exclusionary rule does not apply. *Id.* at 238–39 (quotation marks omitted). This is known as the "good-faith exception" to the exclusionary rule. *Fisher*, 745 F.3d at 203.

The district court denied Ammons' suppression motion because it concluded that the good-faith exception applied. Ammons challenges that conclusion on appeal. He argues that the good-faith exception is categorically inapplicable to warrants that are void *ab initio* for lack of jurisdiction.[1] And, even if the good-faith exception could apply, he argues that the agents' reliance on the Virginia Warrant was objectively unreasonable.

The Virginia Warrant "has implicated more than a hundred defendants across the United States," *United States v. Horton*, 863 F.3d 1041, 1045–46 (8th Cir. 2017) (collecting cases), so it is perhaps unsurprising that this is not our first encounter with a suppression claim like Ammons'. Indeed, in *United States v. Moorehead*, 912 F.3d 963, 967 (6th Cir. 2019), we rejected the same objections to good-faith reliance on the Virginia Warrant that Ammons raises here. *See id*. at 968, 970. *Moorehead*, therefore, forecloses both of Ammons' arguments. In his reply brief, Ammons asks us to disregard *Moorehead* and rely instead on our earlier decision in *United States v. Scott*, which held that the good-faith exception does not apply "whe[n] a warrant is issued by a person lacking the requisite legal authority." 260 F.3d 512, 515 (6th Cir. 2001). But *Moorehead* rejected that argument as well. *See* 912 F.3d at 969 (recognizing that *Scott*'s holding had been modified

[1] Ammons' argument that the Virginia Warrant is void *ab initio* for lack of jurisdiction is based, in part, on the Federal Rules of Criminal Procedure as they existed at the time of the search. Because we conclude that the good-faith exception applies, we need not decide whether the warrant was invalid. We note, however, that the Rules were later amended to expressly authorize warrants like the Virginia Warrant. *See* Fed. R. Crim. P. 41(b)(6) ("[A] magistrate judge having authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district . . . .").

by our decision in *United States v. Master*, 614 F.3d 236, 242–43 (6th Cir. 2010), due to intervening Supreme Court precedent). Accordingly, we affirm the district court's denial of Ammons' suppression motion.

B.

Ammons' sentencing challenge is likewise foreclosed by our precedent. He argues that the enhancements outlined in U.S.S.G. § 2G2.2 are so broadly applicable in child-pornography cases that a sentence premised on those enhancements is substantively unreasonable. He concedes, however, that this argument is directly foreclosed by our decision in *United States v. Lynde*, 926 F.3d 275 (6th Cir. 2019); he nonetheless wishes to preserve this argument for further review. Ammons is right that *Lynde* controls and forecloses his claim to sentencing relief here. *See* 926 F.3d at 279–80.

C.

Finally, Ammons argues that the district court erred in denying his motion for acquittal because the evidence presented at trial was insufficient to prove his guilt beyond a reasonable doubt. This is a question of law that we review de novo. *United States v. Graham*, 622 F.3d 445, 448 (6th Cir. 2010). A defendant claiming evidence insufficiency must meet "a very heavy burden." *United States v. Abboud*, 438 F.3d 554, 589 (6th Cir. 2006) (quoting *United States v. Vannerson*, 786 F.2d 221, 225 (6th Cir. 1986)). We view all evidence "in [the] light most favorable to the prosecution, giving the prosecution the benefit of all reasonable inferences from the testimony." *United States v. McAuliffe*, 490 F.3d 526, 537 (6th Cir. 2007). And we may disturb

the jury's verdict only if no "rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Id.*

Section 2252A(a)(5)(B) forbids "[a]ny person" to "knowingly access[] with intent to view[] any . . . material that contains an image of child pornography." Thus, to convict Ammons, the prosecution had to prove beyond a reasonable doubt that Ammons (1) knowingly accessed with intent to view, (2) any material, (3) that he knew contained an image of child pornography. *See United States v. Brune*, 767 F.3d 1009, 1020 (10th Cir. 2014).

Ammons attempts to refute the first element. He points to the fact that the images containing child pornography were found in his web browser's cache. Cache is a storage drive used by web browsers, like Google Chrome, to locally save web pages visited by a user. By storing this information, cache allows web browsers to more quickly load web content. Importantly, though, not all content stored in cache has necessarily been seen by the user. For example, when a page on a website requires users to scroll down to see more content, all of the page's content is stored in cache even if the user never scrolls to the bottom of the page. Additionally, material from external websites linked to the website being viewed may be stored in cache in anticipation that the user might click on the link. Because it is technically possible that the 220 images of child pornography found in Ammons' cache were stored without him viewing the material, Ammons contends that no rational juror could have found him guilty beyond a reasonable doubt.

We disagree. First, Ammons' argument relies on a false premise. A conviction under § 2252A(a)(5)(B) does not require the defendant to have actually viewed the illegal images. *See Tagg*, 886 F.3d at 587. "The access-with-intent offense is complete the moment that the elements of access and intent coincide." *Id.* Thus, the jury could have convicted Ammons if it found that he knowingly accessed a child-pornography website with intent to view illicit images, but stopped

short of actually viewing the images. *Id.* ("[E]ven if the person never viewed illegal child pornography, knowingly accessing a child-pornography website with the intent to view illegal materials is itself a criminal act.").

Second, the government presented ample evidence at trial from which a rational juror could find Ammons guilty—even under Ammons' own theory of § 2252A(a)(5)(B). Agents Brian Coyt and Virginia MacHenry, who interviewed Ammons after the search, testified that Ammons admitted to viewing child pornography while browsing the internet. More specifically, the agents said that Ammons admitted to installing the Tor software on his browser and encountering child pornography on the dark web. The agents then explained that these websites on the dark web could not be accessed through a traditional Google search, but instead had to be intentionally sought out using the Tor software. Finally, Agent MacHenry testified that Ammons had admitted to browsing forums on the traditional internet, such as 4chan, which "told him certain locations on TOR to look for child pornography." R. 125, PageID 866. While Ammons testified that the agents were misrepresenting his statements during the interview, the jury was not required to credit his testimony.

The prosecution also presented the testimony of Agent Amanda Rankhorn, the forensic specialist who analyzed Ammons' hard drive. Agent Rankhorn testified that, at 8:08 AM on October 22, 2015, Ammons had entered a Google search for the term "jblover." Rankhorn then testified that the browser cache indicated that Ammons had visited the website "jblover.org," which included forums titled, "Jailbait forum – Stickam Captures – Omegle Captures." And she explained that many of the 220 images of child pornography found in Ammons' cache contained a logo for "omegle.com," a video-chatting website. Finally, Rankhorn testified that most of the images showed young girls with their legs spread apart exposing their genitals—which matched

testimony provided by Ammons' niece, who told the jury that Ammons had forced her to pose in the identical position. A sealed exhibit submitted to the jury contained a sample of 10 of the 220 images found on Ammons' hard drive. Taking this evidence in the light most favorable to the prosecution, a "rational trier of fact" certainly could have found Ammons guilty beyond a reasonable doubt. *See Graham*, 622 F.3d at 448.

* * *

For the foregoing reasons, the judgment of the district court is AFFIRMED.